Professor Messer

Professor Messer's

CompTIA SECURITY+

SY0-501

Course Notes

James "Professor" Messer

Professor Messer's CompTIA SY0-501 Security+ Course Notes

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's CompTIA SY0-501 Security+ Course Notes
Written by James "Professor" Messer

http://www.ProfessorMesser.com

First Edition: October 2017
This is version 1.93

Trademark Acknowledgments

Warning and Disclaimer
This book is designed to provide information about the CompTIA SY0-501 Security+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Contents

Introduction

Information technology security is a significant concern for every IT specialist. Our systems are under constant attack, and the next generation of security professionals will be at the forefront of keeping our critical information safe.

CompTIA's Security+ exam tests you on the specifics of network security, vulnerabilities and threats, cryptography, and much more. I've created these Course Notes to help you through the details that you need to know for the exam. Best of luck with your studies!

- Professor Messer

The CompTIA Security+ certification

To earn the Security+ certification, you must pass a single SY0-501 certification exam. The exam is 90 minutes in duration and includes both multiple choice questions and performance-based questions. Performance-based questions can include fill-in-the-blank, matching, sorting, and simulated operational environments. You will need to be very familiar with the exam topics to have the best possible exam results.

Here's the breakdown of each technology section and the percentage of each topic on the SY0-501 exam:

Section 1.0 - Threats, Attacks, and Vulnerabilities - 21%
Section 2.0 - Technologies and Tools - 22%
Section 3.0 - Architecture and Design - 15%
Section 4.0 - Identity and Access Management - 16%
Section 5.0 - Risk Management - 14%
Section 6.0 - Cryptography and PKI - 12%

CompTIA provides a detailed set of exam objectives that provide a list of everything you need to know before you take your exam. You can find a link to the exam objectives here:

http://www.professormesser.com/objectives/

How to use this book

Once you're comfortable with all of the sections in the official CompTIA SY0-501 exam objectives, you can use these notes as a consolidated summary of the most important topics. These Course Notes follow the same format and numbering scheme as the official exam objectives, so it should be easy to cross reference these notes with the Professor Messer video series and all of your other study materials.


Professor
Messer

Professor Messer's

CompTIA Security+

SY0-501 Course Notes

http://www.ProfessorMesser.com

1.1 - An Overview of Malware

Malware

- Malicious software - These can be very bad
- Gather information - Keystrokes
- Participate in a group - Controlled over the 'net
- Show you advertising - Big money
- Viruses and worms
  - Encrypt your data
  - Ruin your day

Malware types and methods

- Viruses
- Crypto-malware, Ransomware
- Worms
- Trojan Horse
- Rootkit
- Keylogger
- Adware/Spyware
- Botnet

How you get malware

- These all work together
  - A worm takes advantage of a vulnerability
  - Installs malware that includes a remote access backdoor
  - Bot may be installed later
- Your computer must run a program
  - Email link
  - Don't click links
  - Web page pop-up
  - Drive-by download
  - Worm
- Your computer is vulnerable
  - Operating system
  - Keep your OS updated!
  - Application
  - The Adobe Flash vulnerability of the moment

1.1 - Viruses and Worms

Virus

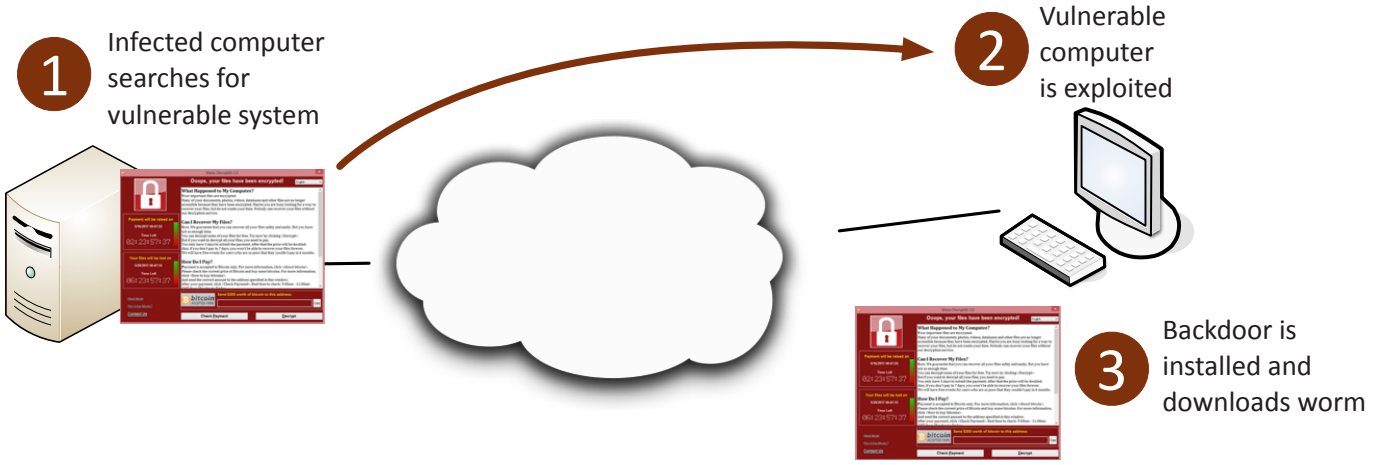
- Malware that can reproduce itself
  - It doesn't need you to click anything
  - It needs you to execute a program
- Reproduces through file systems or the network
  - Just running a program can spread a virus
- May or may not cause problems
  - Some viruses are invisible, some are annoying
- Anti-virus is very common
  - Thousands of new viruses every week
  - Is your signature file updated?

Types of Viruses

- Program viruses - It's part of the application
- Boot sector viruses - Who needs an OS?
- Script viruses - Operating system and browser-based
- Macro viruses - Common in Microsoft Office

Worms

- Malware that self-replicates
  - Doesn't need you to do anything
  - Uses the network as a transmission medium
  - Self-propagates and spreads quickly
- Worms are pretty bad things
  - Can take over many systems very quickly
- Firewalls and IDS/IPS can mitigate many worm infestations
  - Doesn't help much once the worm gets inside



1.1 - Ransomware and Crypto-Malware

Your data is valuable

- Personal data
  - Family pictures and videos
  - Important documents
- Organization data
  - Planning documents
  - Employee personally identifiable information (PII)
  - Financial information
  - Company private data
- How much is it worth?
  - There's a number

Ransomware

- The bad guys want your money
  - They'll take your computer in the meantime
- Probably a fake ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional may be able to remove these kinds of malware

Crypto-malware

- New generation of ransomware
  - Your data is unavailable until you provide cash
- Malware encrypts your data files
  - Pictures, documents, music, movies, etc.
  - Your OS remains available
  - They want you running, but not working
- You must pay the bad guys to obtain the decryption key
  - Untraceable payment system
  - An unfortunate use of public-key cryptography

Protecting against ransomware

- Always have a backup - an offline backup, ideally
- Keep your operating system up to date
  - Patch those vulnerabilities
- Keep your applications up to date
  - Security patches
- Keep your anti-virus/anti-malware signatures up to date
  - New attacks every hour
- Keep everything up to date.

1.1 - Trojans and RATs

Trojan horse

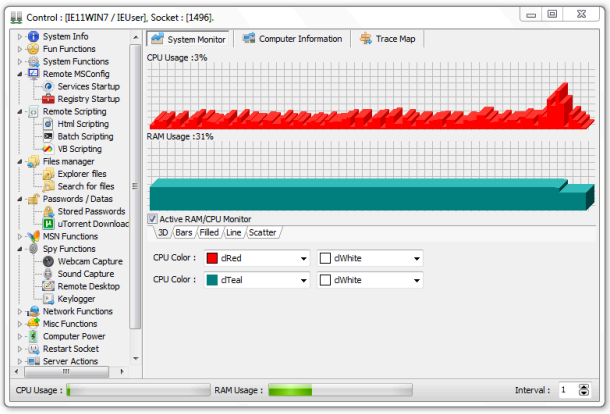
- Used by the Greeks to capture Troy from the Trojans
  - A digital wooden horse
- Software that pretends to be something else
  - So it can conquer your computer
  - Doesn't really care much about replicating
- Circumvents your existing security
  - Anti-virus may catch it when it runs
- The better Trojans are built to avoid and disable AV
- Once it's inside it has free reign
  - And it may open the gates for other programs

Backdoors

- Why go through normal authentication methods?
  - Just walk in the back door
- Often placed on your computer through malware
  - Some malware software can take advantage of backdoors created by other malware
- Some software includes a backdoor
  - Old Linux kernel included a backdoor
  - Bad software can have a backdoor as part of the app

Remote Access Trojans (RATs)

- Remote Administration Tool
  - The ultimate backdoor
  - Administrative control of a device
- Malware installs the server/service/host
  - Bad guys connect with the client software
- Control a device
  - Key logging, screen recording /screenshots, copy files
- Embed more malware



1.1 - Rootkits

Rootkits

- Originally a Unix technique
  - The "root" in rootkit
- Modifies core system files
  - Part of the kernel
- Can be invisible to the operating system
  - Won't see it in Task Manager
- Also invisible to traditional anti-virus utilities
  - If you can't see it, you can't stop it

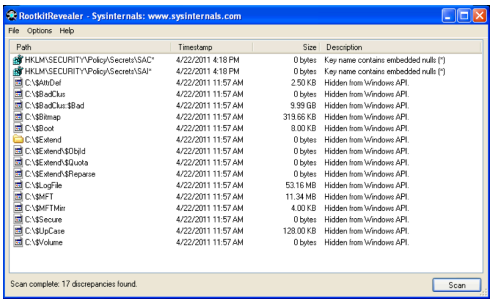
Kernel drivers

- Zeus/Zbot malware
  - Famous for cleaning out bank accounts
- Now combined with Necurs rootkit
  - Necurs is a kernel-level driver
- Necurs makes sure you can't delete Zbot
  - Access denied
- Trying to stop the Windows process?
  - Error terminating process: Access denied

1.1 - Rootkits (continued)

Finding and Removing rootkits

- Look for the unusual
  - Anti-malware scans
- Use a remover specific to the rootkit
  - Usually built after the rootkit is discovered
- Secure boot with UEFI
  - Security in the BIOS



1.1 - Keyloggers

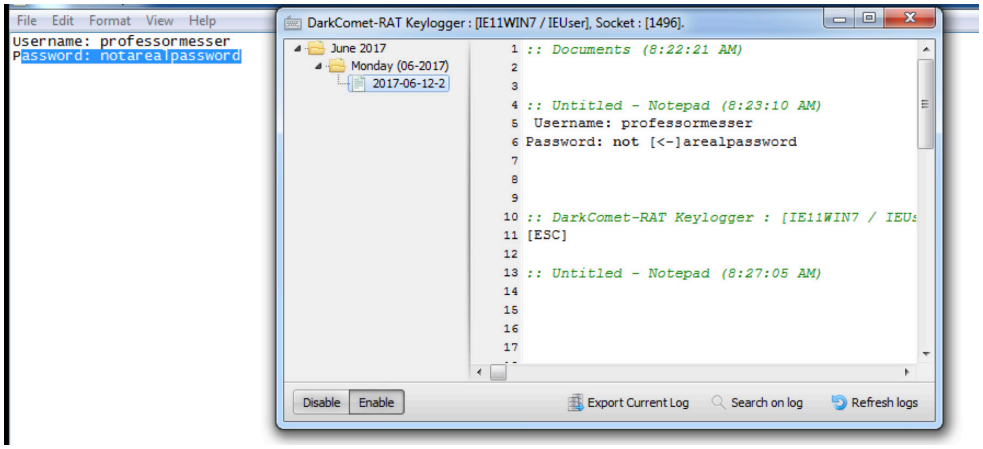
Keyloggers

- Your keystrokes contain valuable information
  - Web site login URLs, passwords, email messages
- Save all of your input
  - Send it to the bad guys
- Circumvents encryption protections
  - Your keystrokes are in the clear
- Other data logging
  - Clipboard logging, screen logging, instant messaging, search engine queries

Preventing Keyloggers

- Usually installed with malware
  - Use anti-virus/anti-malware
  - Keep your signatures updated
- Block unauthorized communication
  - Block the exfiltration attempt
  - Firewall rules / monitoring
- Run a keylogging scanner
  - Checks for keylogging activity

DarkComet-RAT Keylogger



1.1 - Adware and Spyware

Adware

- Your computer is one big advertisement
  - Pop-ups with pop-ups
- May cause performance issues
  - Especially over the network
- Installed accidentally
  - May be included with other software installations
- Be careful of software that claims to remove adware
  - Especially if you learned about it from a pop-up

Spyware

- Malware that spies on you
  - Advertising, identity theft, affiliate fraud
- Can trick you into installing
  - Peer to peer, fake security software
- Browser monitoring - Capture surfing habits
- Keyloggers
  - Capture every keystroke, send it back to the mother ship

Why is there so much adware and spyware?

- Money - Your eyeballs are incredibly valuable
- Money - Your computer time and bandwidth is incredibly valuable
- Money - Your bank account is incredibly valuable

Protecting against adware/spyware

- Maintain your anti-virus / anti-malware
  - Always have the latest signatures
- Always know what you're installing
  - And watch your options during the installation
- Where's your backup?
  - You might need it someday
  - Cleaning adware isn't easy
- Run some scans
  - Malwarebytes

1.1 - Bots and Botnets

Botnets

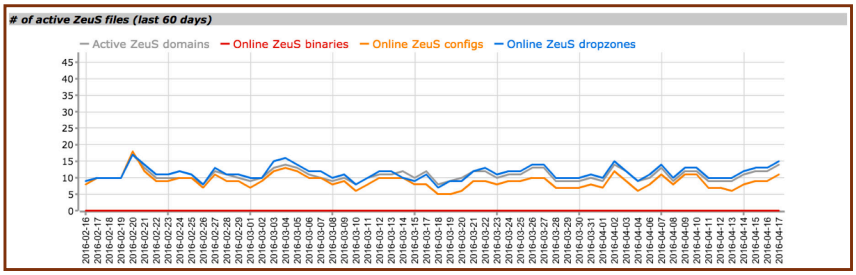
- Robot networks
  - Skynet is self-aware
- Once your machine is infected, it becomes a bot
  - You may not even know
- How does it get on your computer?
  - Trojan Horse (I just saw a funny video of you! Click here.)
    You run a program or click an ad you THOUGHT was legit, but...
  - OS or application vulnerability
- A day in the life of a bot
  - Sit around. Check in with the mother ship. Wait for instructions.

Botnets

- A group of bots working together
  - Nothing good can come from this
- Distributed Denial of service (DDoS)
  - The power of many
- Botnets are for sale
  - Rent time from the bad guys
  - Not a long-term business proposition

Stopping the Bots

- Prevent the initial infection
  - OS and application patches
  - Anti-virus/anti-malware and updated signatures
- Identify an existing infection
  - On-demand scans
  - Network monitoring
- Prevent command and control (C&C)
  - Block at the firewall
  - Identify at the workstation with a host-based firewall or host-based IPS



1.1 - Logic Bombs

Logic bomb

- Waits for a predefined event
  - Often left by someone with grudge
- Time bomb - Time or date
- User event - Logic bomb
- Difficult to identify
  - Difficult to recover if it goes off

Real world logic bombs

- March 19, 2013, South Korea
  - Email with malicious attachment sent to South Korean organizations
  - Posed as a bank email
  - Trojan installs malware
- March 20, 2013, 2 p.m. local time
  - Malware logic-bomb activates
  - Storage and master boot record deleted, system reboots
- Boot device not found.
  - Please install an operating system on your hard disk.

Real world logic bombs

- December 17, 2016, 11:53 p.m.
- Kiev, Ukraine, high-voltage substation
- Logic bomb begins disabling electrical circuits
  - Malware mapped out the control network
- Began disabling power at a predetermined time
- Customized for SCADA networks
  - Supervisory Control and Data Acquisition

Preventing a logic bomb

- Difficult to recognize
  - Each is unique - No predefined signatures
- Process and procedures
  - Formal change control
- Electronic monitoring
  - Alert on changes
  - Host-based intrusion detection, Tripwire, etc.
- Constant auditing
  - An administrator can circumvent existing systems

1.2 - Phishing

Phishing

- Social engineering with a touch of spoofing

Check the URL

- Usually there's something not quite right
  - Spelling, fonts, graphics
- Vishing is done over the phone
  - Fake security checks or bank updates

Spearfishing

- Phishing with inside information
  - Makes the attack more believable
  - Spear phishing the CEO is "whaling"
- April 2011 - Epsilon
  - Less than 3,000 email addresses attacked
  - 100% of email operations staff
  - Downloaded anti-virus disabler, keylogger, and remote admin tool
- April 2011 - Oak Ridge National Laboratory
  - Email from the "Human Resources Department"
  - 530 employees targeted, 57 clicked, 2 were infected
  - Data downloaded, servers infected with malware

1.2 - Phishing (continued)

The big phish
- March 19, 2016
- John Podesta, Former White House Chief of Staff, Former Counselor to the President of the United States
- Former chairman of the 2016 Hillary Clinton United States presidential campaign
- Gmail personal account with messages from 2007 through 2016

Filling the net
- Podesta used the bit.ly link in the email to "reset" his password
  - Wasn't actually a Google reset link
- Ten years of personal emails were unlocked
  - And downloaded
- Every email was made available on WikiLeaks
  - The good, the bad, and the ugly
- Don't underestimate the effects of phishing
  - It can have significant repercussions

1.2 - Tailgating and Impersonation

Tailgating
- Use someone else to gain access to a building
  - Not an accident
- Johnny Long / No Tech Hacking
  - Blend in with clothing
  - 3rd-party with a legitimate reason
  - Temporarily take up smoking
  - I still prefer bringing doughnuts
- Once inside, there's little to stop you
  - Most security stops at the border

Watching for tailgating
- Policy for visitors
  - You should be able to identify anyone
- One scan, one person
  - A matter of policy or mechanically required
- Mantrap / Airlock
  - You don't have a choice
- Don't be afraid to ask
  - Who are you and why are you here?

Impersonation
- Pretend to be someone you aren't
  - Halloween for the fraudsters
- Use some of those details you got from the dumpster
  - You can trust me, I'm with your help desk
- Attack the victim as someone higher in rank
  - Office of the Vice President for Scamming
- Throw tons of technical details around
  - Catastrophic feedback due to the depolarization of the differential magnetometer
- Be a buddy - How about those Cubs?

Protect against Impersonation
- Never volunteer information - My password is 12345
- Don't disclose personal details - The bad guys are tricky
- Always verify before revealing info
  - Call back, verify through 3rd parties
- Verification should be encouraged
  - Especially if your organization owns valuable information

1.2 - Dumpster Diving

Dumpster Diving
- Mobile garbage bin
  - United States brand name "Dumpster"
  - Similar to a rubbish skip
- Important information thrown out with the trash
  - Thanks for bagging your garbage for me!
- Gather details that can be used for a different attack
  - Impersonate names, use phone numbers
- Timing is important
  - Just after end of month, end of quarter
  - Based on pickup schedule

Is it legal to dive in a dumpster?
- I am not a lawyer.
- In the United States, it's legal
  - Unless there's a local restriction
- If it's in the trash, it's open season
  - Nobody owns it
- Dumpsters on private property or "No Trespassing" signs may be restricted
  - You can't break the law to get to the rubbish
- Questions? Talk to a legal professional.
- Secure your garbage
  - Fence and a lock

Protect your rubbish
- Shred your documents
  - This will only go so far
  - Governments burn the good stuff
- Go look at your trash
  - What's in there?

1.2 - Shoulder Surfing

Shoulder Surfing

- You have access to important information
  - Many people want to see
  - Curiosity, industrial espionage, competitive advantage
- This is surprisingly easy
  - Airports / Flights, hallway-facing monitors, coffee shops
- Surf from afar
  - Binoculars / Telescopes, webcam monitoring

Preventing shoulder surfing

- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways
- Don't sit in front of me on your flight
  - I can't help myself

1.2 - Hoaxes

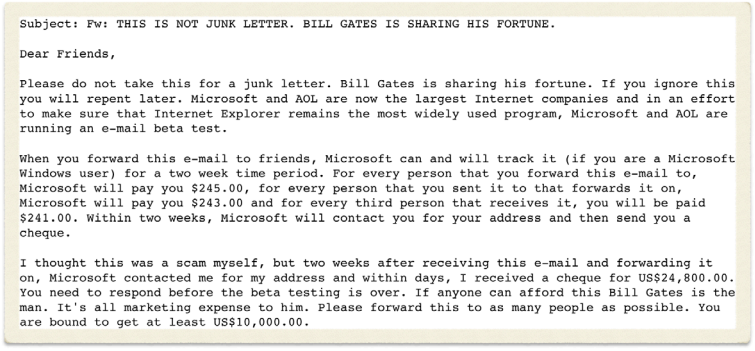
Computer hoaxes

- A threat that doesn't actually exist
  - But they seem like they COULD be real
- Still often consume lots of resources
  - Forwarded email messages, printed memorandums, wasted time
- Often an email - Or Facebook wall post, or tweet, or...
- Some hoaxes will take your money
  - But not through electronic means
- A hoax about a virus can waste as much time as a regular virus

De-hoaxing

- It's the Internet. Believe no one.
  - Consider the source
- Cross reference
  - http://www.hoax-slayer.net
  - http://www.snopes.com
- Spam filters can help
- If it sounds too good to be true...
  - So many sad stories

Hoax Examples



Subject: Fw: THIS IS NOT JUNK LETTER. BILL GATES IS SHARING HIS FORTUNE.

Dear Friends,

Please do not take this for a junk letter. Bill Gates is sharing his fortune. If you ignore this you will repent later. Microsoft and AOL are now the largest Internet companies and in an effort to make sure that Internet Explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test.

When you forward this e-mail to friends, Microsoft can and will track it (if you are a Microsoft Windows user) for a two week time period. For every person that you forward this e-mail to, Microsoft will pay you $245.00, for every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, you will be paid $241.00. Within two weeks, Microsoft will contact you for your address and then send you a cheque.

I thought this was a scam myself, but two weeks after receiving this e-mail and forwarding it on, Microsoft contacted me for my address and within days, I received a cheque for US$24,800.00. You need to respond before the beta testing is over. If anyone can afford this Bill Gates is the man. It's all marketing expense to him. Please forward this to as many people as possible. You are bound to get at least US$10,000.00.

1.2 - Watering Hole Attacks

Watering Hole Attack

- What if your network was really secure?
  - You didn't even plug in that USB key from the parking lot
- The bad guys can't get in
  - Not responding to phishing emails
  - Not opening any email attachments
- Have the mountain come to you
  - Go where the mountain hangs out
  - The watering hole
  - This requires a bit of research

Executing the water hole attack

- Determine which website the victim group uses
  - Educated guess - Local coffee or sandwich shop
  - Industry-related sites
- Infect one of these third-party sites
  - Site vulnerability, email attachments
- Infect all visitors
  - But you're just looking for specific victims

Because that's where the money is

- January 2017
- Polish Financial Supervision Authority, National Banking and Stock Commission of Mexico, State-owned bank in Uruguay
  - The watering hole was sufficiently poisoned
- Visiting the site would download malicious JavaScript files
  - But only to IP addresses matching financial institutions
- Did the attack work? We still don't know

Watching the watering hole

- Defense-in-depth
  - Layered defense
  - It's never one thing
- Firewalls and IPS
  - Stop the network traffic before things get bad
- Anti-virus / Anti-malware signature updates
  - The Polish Financial Supervision Authority attack code was recognized and stopped by generic signatures in Symantec's anti-virus software

1.2 - Principles of Social Engineering

Effective social engineering

- Constantly changing
  - You never know what they'll use next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or association

Social engineering principles

- Authority
  - The social engineer is in charge
  - I'm calling from the help desk/office of the CEO/police
- Intimidation
  - There will be bad things if you don't help
  - If you don't help me, the payroll checks won't be processed
- Consensus / social proof
  - Convince based on what's normally expected
  - Your co-worker Jill did this for me last week
- Scarcity
  - The situation will not be this way for long
  - Must make the change before time expires
- Urgency
  - Works alongside scarcity
  - Act quickly, don't think
- Familiarity / liking
  - Someone you know, we have common friends
- Trust
  - Someone who is safe
  - I'm from IT, and I'm here to help

How I lost $50,000 Twitter Username

- Naoki Hiroshima - @N
  - https://medium.com/cyber-security/24eb09e026dd
- Bad guy calls PayPal and uses social engineering to get the last four digits of the credit card on file
- Bad guy calls GoDaddy and tells them he lost the card, so he can't properly validate. But he has the last four, does that help?
  - GoDaddy let the bad guy guess the first two digits of the card
  - He was allowed to keep guessing until he got it right
  - Social engineering done really, really well

How to steal $50,000 Twitter name

- Bad guy is now in control of every domain name
  - And there were some good ones
- Bad guy extorts a swap
  - Domain control for @N
  - Owner agrees
- Twitter reviewed the case for a month
  - Eventually restored access to @N

1.2 - Denial of Service

Denial of Service

- Force a service to fail
  - Overload the service
- Take advantage of a design failure or vulnerability
  - Keep your systems patched!
- Cause a system to be unavailable
  - Competitive advantage
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack
- Doesn't have to be complicated
  - Turn off the power

A "friendly" DoS

- Unintentional DoSing
  - It's not always a ne'er-do-well
- Network DoS - Layer 2 loop without STP
- Bandwidth DoS - Downloading multi-gigabyte Linux distributions over a DSL line
- The water line breaks
  - Get a good shop vacuum

Distributed Denial of Service (DDoS)

- Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
- This is why the bad guys have botnets
  - Thousands or millions of computers at your command
  - At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- Asymmetric threat
  - The attacker may have fewer resources than the victim

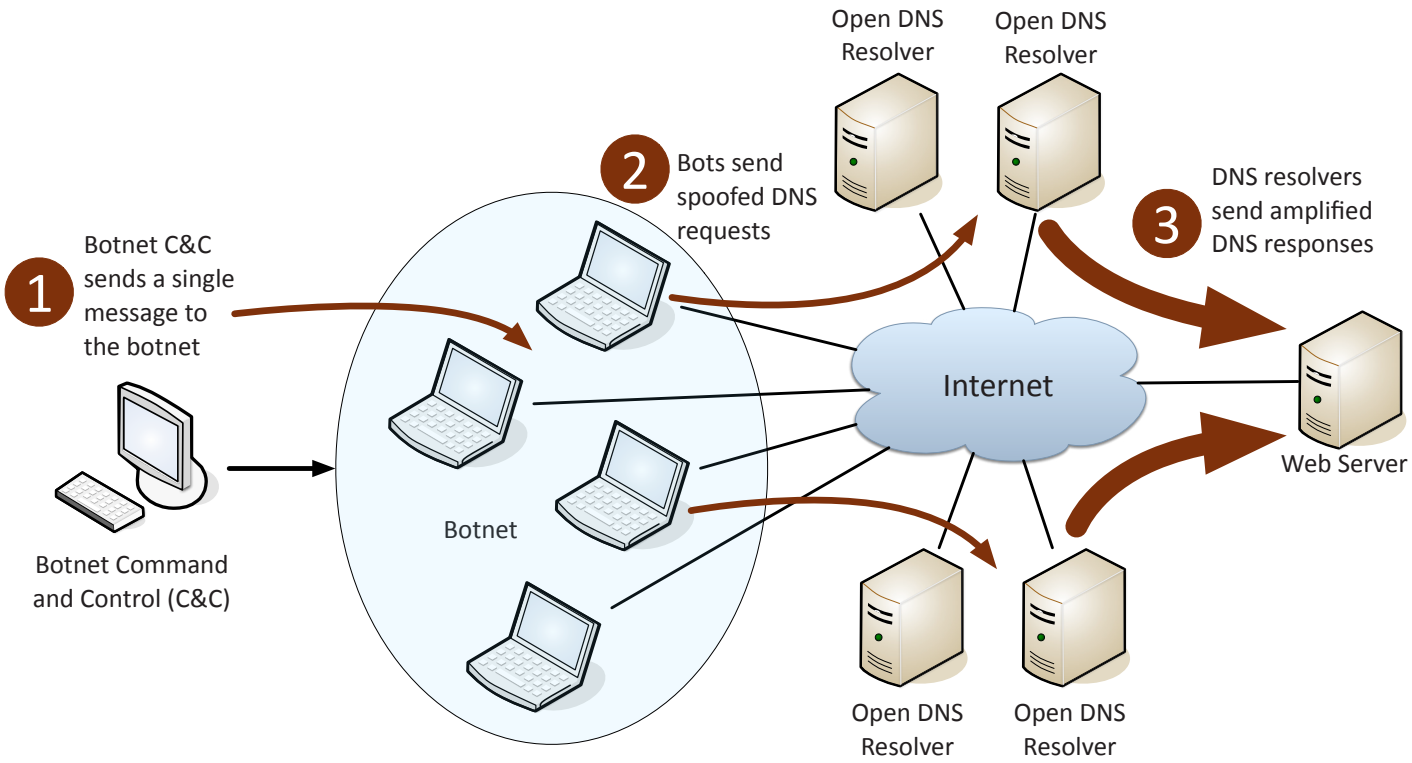
DDoS amplification

- Turn your small attack into a big attack
  - Often reflected off another device or service
- An increasingly common DDoS technique
  - Turn Internet services against the victim
- Uses protocols with little (if any) authentication or checks
  - NTP, DNS, ICMP
  - A common example of protocol abuse

Example of a DNS record used in DDoS amplification attack

```
$ dig ANY isc.org @75.75.75.75
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.8.3-P1 <<>> ANY isc.org @75.75.75.75
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27443
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;isc.org.                       IN      ANY

;; ANSWER SECTION:
isc.org.                1712    IN      DNSKEY  257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMvoOMRXjGr
hhCeFvAZih7yJHf8ZGfW6hd38hXG/xylYCO6Krpbdojwx8YMXLA5/kA+ u50WIL8ZR1R6KTbsYVMf/
Qx5RiNbPClw+vT+U8eXEJmO20jIS1ULgqy3 47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz
Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyL KOOedS39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmw3oA8lVUgEf/
rzeC/bB yBNsO70aEFTd
isc.org.                1712    IN      DNSKEY  256 3 5 AwEAAbDs5ksq3roEgvfiN+HHzPqErVe5lOpQ6bNjRDH/
BSUisBM8gvgd ZGIdctVRYl8vgAJcpc//YE4vpNrDsfgGfiyz+Fd2pCJTXGm6mDoAAMLJ
FrG64gYVdby2AnI7sonZlT5PHjS0dKBhhf0Pd/+SgKNIf25wh1UzFRCp CXznWdER
isc.org.                1712    IN      RRSIG   DNSKEY 5 2 7200 20170712230419 20170612230419
12892 isc.org. MZ8PU+4k/wwHDw3jdyzUpm74MFhbFvCemlJ61ho0gkDGNhEqn8/yC1Fs oaT7PK9U8hknlrppp/
os08yUifegPsvO1mhezTfIEHTP+JPJS6VO0G5A a9QHQtVO2FOPuR7HW2AQysldFL9pfvwOlKkzm4yuuhrM2BqhMeSZimo6
VvolWqHyE58dOHoyeylmcvmNb45qoR4spKZR9A1hdxesYgI1tosw9tTd
PswnkyO3rizmFjABzcXDUeKSlodPRr1hZd6rNRRacIeiskPxw8E6WTnT
0RzOM7nFBDIKeTixA59xlPpIN2t+xh1zu8tQ5NsMF2CJK+b5LZTjovEg 9ho9NA==
isc.org.                1712    IN      RRSIG   DNSKEY 5 2 7200 20170712230419 20170612230419 60321 isc.
org. fVnJffUYaDDrUYbo4hhPwKzjyzB6QEExLWao5jyaIDpEYL/aymTk6/51 nAubio2qdlgFinpoHmkaRDVdV1DG/6CWmA2/
tVAzSs77+qw3KkEYJbNq IR/bgkhxPtti/7+65YrPZ9yrNiPpB5LbNTmJyeuuQD4camliS9qHnlv6 618=

;; Query time: 13 msec
;; SERVER: 75.75.75.75#53(75.75.75.75)
;; WHEN: Fri Jun 16 17:36:51 2017
;; MSG SIZE  rcvd: 912
```

DNS Amplification



1.2 - Man-in-the-Middle / On-path attacks

Man -in- the-middle / On-path attack

- How can a bad guy watch without you knowing?
  - Man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - ARP has no security

Man-in-the-browser / On-path attack

- What if the middleman was on the same computer as the victim?
  - The calls are coming from inside the browser!
  - Malware/Trojan does all of the proxy work
- Huge advantages for the bad guys
  - Relatively easy to proxy encrypted traffic
  - Everything looks normal to the victim
- The man-in-the-browser waits for you to login to your bank
  - And cleans you out

1.2 - Buffer Overflows

Buffer Overflows

- Overwriting a buffer of memory
  - Spills over into other memory areas
- Developers need to perform bounds checking
  - The bad guys spend a lot of time looking for openings
- Not a simple exploit
  - Takes time to avoid crashing things
  - Takes time to make it do what you want
- A really useful buffer overflow is repeatable
  - Which means that all systems are owned

Variable A and B before buffer overflow

Variable Name	A								B	
Value	[null string]								1979	
Hex Value	00	00	00	00	00	00	00	00	07	BB

Overflowing variable A changes variable B

Variable Name	A								B	
Value	'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	25856	
Hex Value	65	78	63	65	73	73	69	76	65	00

1.2 - Data Injection

Code Injection

- Code injection
  - Adding your own information into a data stream
- Enabled because of bad programming
  - The application should properly handle input and output
- So many different data types
  - HTML, SQL, XML, LDAP, etc.

SQL Injection

- SQL - Structured Query Language
  - The most common relational database management system language
- SQL Injection
  - Modifying SQL requests
  - Your application shouldn't really allow this

XML injection and LDAP injection

- XML - Extensible Markup Language
  - A set of rules for data transfer and storage XML injection
  - Modifying XML requests
  - A good application will validate
- LDAP - Lightweight Directory Access Protocol
  - Created by the telephone companies
  - Now used by almost everyone
- LDAP injection
  - Modify LDAP requests to manipulate application results

1.2 - Cross-site Scripting - XSS

Cross-Site Scripting

- XSS
  - Cascading Style Sheets (CSS) are something else entirely
- Originally called cross-site because of browser security flaws
  - Information from one site could be shared with another
- One of the most common web application development errors
  - Takes advantage of the trust a user has for a site
  - Complex and varied
- Malware that uses JavaScript
  - Do you allow scripts? Me too.

Non-persistent (reflected) XSS attack

- Web site allows scripts to run in user input
  - Search box is a common source
- Bad guy emails a link that takes advantage of this vulnerability
  - Runs a script that sends credentials/session IDs/ cookies to the bad guy
- Script embedded in URL executes in the victim's browser
  - As if it came from the server
- Bad guys uses credentials/session IDs/ cookies to steal victim's information without their knowledge
  - Very sneaky

1.2 - Cross-site Scripting - XSS (continued)

Persistent (stored) XSS attack
- Bad guy posts a message to a social network
  - Includes the malicious payload
- It's now "persistent"
  - Everyone gets the payload
- No specific target
  - All viewers to the page
- For social networking, this can spread quickly
  - Everyone who views the message can have it posted to their page
  - Where someone else can view it and propagate it further...

Hacking a Subaru
- June 2017, Aaron Guzman
  - Security researcher
- When authenticating with Subaru, users get a token
  - This token never expires (bad!)
- A valid token allowed any service request
  - Even adding your email address to someone else's account
  - Now you have full access to someone else's car
- Web front-end included an XSS vulnerability
  - A user clicks a malicious link, and you have their token
  - Web server and browser-based applications

Protecting against XSS
- Be careful when clicking untrusted links
  - Never blindly click in your email inbox. Never.
- Consider disabling JavaScript
  - Or control with an extension
  - This offers limited protection
- Keep your browser and applications updated
  - Avoid the nasty browser vulnerabilities
- Validate input
  - Don't allow users to add their own scripts to an input field

1.2 - Cross-site Request Forgery

Cross-site request forgery
- One-click attack, session riding
  - XFRF, CSRF (sea surf)
- Takes advantage of the trust that a web application has for the user
  - The web site trusts your browser
- Significant web application development oversight
  - The application should have anti-forgery techniques added
  - Usually a cryptographic token to prevent a forgery

1.2 - Privilege Escalation

Privilege escalation
- Gain higher-level access to a system
  - Exploit a vulnerability
  - Might be a bug or design flaw
- Higher-level access means more capabilities
  - This commonly is the highest-level access
  - This is obviously a concern
- These are high-priority vulnerability patches
  - You want to get these holes closed very quickly
  - Any user can be an administrator
- Horizontal privilege escalation
  - User A can access user B resources

Mitigating privilege escalation
- Patch quickly
  - Fix the vulnerability
- Updated anti-virus/anti-malware software
  - Block known vulnerabilities
- Data Execution Prevention
  - Only data in executable areas can run
- Address space layout randomization
  - Prevent a buffer overrun at a known memory address

1.2 - DNS Poisoning and Domain Hijacking

DNS poisoning
- Modify the DNS server
  - Requires some crafty hacking
- Modify the client host file
  - The host file takes precedent over DNS queries
- Send a fake response to a valid DNS request
  - Requires a redirection of the original request or the resulting response

Domain hijacking
- Get access to the domain registration, and you have control where the traffic flows
  - You don't need to touch the actual servers
  - Determines the DNS names and DNS IP addresses
- Many ways to get into the account
  - Brute force
  - Social engineer the password
  - Gain access to the email address that manages the account
  - The usual things

Domain hijacking
- Saturday, October 22, 2016, 1 PM
- Domain name registrations of 36 domains are changed
  - Brazilian bank
  - Desktop domains, mobile domains, and more
- Under hacker control for 6 hours
  - The bad guys became the bank
- 5 million customers, $27 billion in assets
  - Results of the hack have not been publicly released

1.2 - Zero-day Attacks

Zero-day attacks

- Many applications have vulnerabilities
  - We've just not found them yet
- Someone is working hard to find the next big vulnerability
  - The good guys share these with the developer
- Bad guys keep these yet-to-be-discovered holes to themselves
  - They want to use these vulnerabilities for personal gain
- Zero-day
  - The vulnerability has not been detected or published
  - Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE)
  - http://cve.mitre.org/

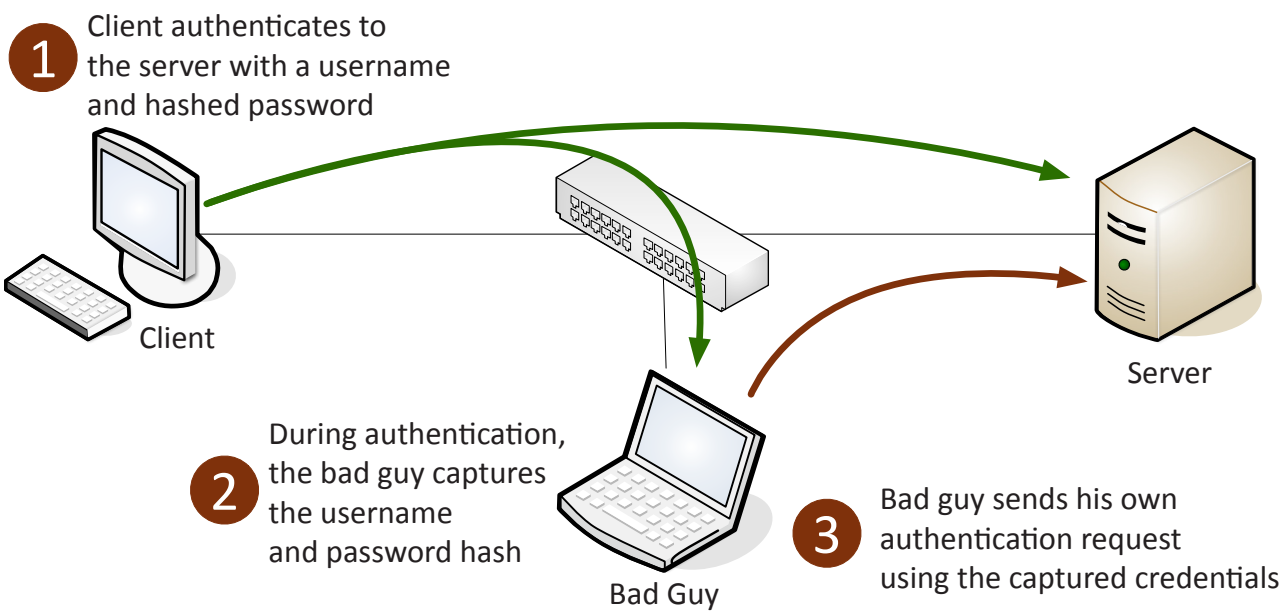
Zero-day vulnerabilities

- March 2017
  - CVE-2017-0199 - Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API
  - Open a Microsoft Office or WordPad file
  - SophosLabs documented attacks in the wild since November 2016
- June 2017
  - CVE-2017-8543 | Windows Search Remote Code Execution Vulnerability
  - Send a specially crafted SMB message to the Search service
  - Install programs, view/change/delete data, create new user accounts

1.2 - Replay Attacks

Replay attack

- Useful information is transmitted over the network
  - A crafty hacker will take advantage of this
- Need access to the raw network data
  - Network tap, ARP poisoning, malware on the victim computer
- The gathered information may help the bad guy
  - Replay the data to appear as someone else
- This is not a MitM attack
  - The actual replay doesn't require the original workstation
- Avoid this type of replay attack with a salt
  - Use a session ID with the password hash to create a unique authentication hash each time



1.2 - Client Hijacking Attacks

URL Hijacking

- Make money from your mistakes
  - There's a lot of advertising on the 'net
- Sell the badly spelled domain to the actual owner
  - Sell a mistake
- Redirect to a competitor
  - Not as common, legal issues
- Phishing site
  - Looks like the real site, please login
- Infect with a drive-by download
  - You've got malware!

Types of URL hijacking

- Typosquatting / brandjacking
  - Take advantage of poor spelling
- Outright misspelling
  - professormesser.com vs. professermesser.com
- A typing error
  - professormeser.com
- A different phrase
  - professormessers.com
- Different top-level domain
  - professormesser.org

1.2 - Client Hijacking Attacks

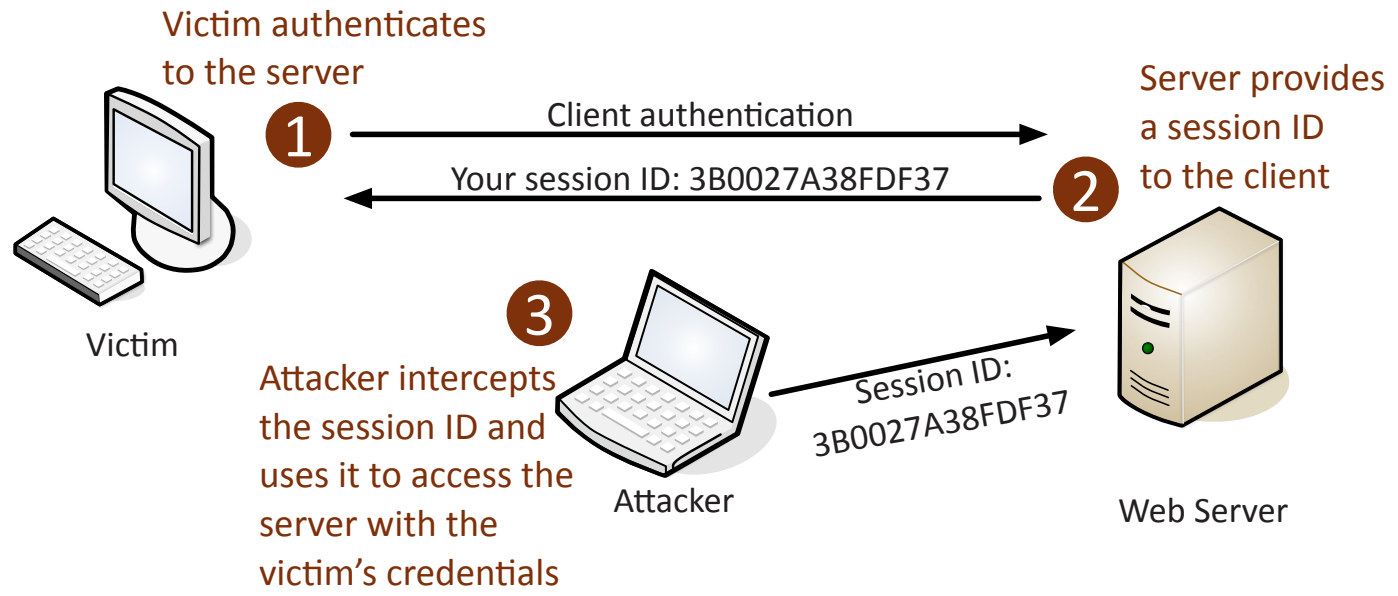
Clickjacking
- You're clicking on a button
  - But you're actually clicking on something else
- Normal web page underneath
  - Invisible layer on the top

Clickjacking your phone
- May 2017
  - Georgia Institute of Technology report
- Cloak & Dagger
  - Android OS up to version 7.1.2
- Invisible information drawn over the screen
  - Monitor keystrokes and record user input

Browser cookies and session ID's
- Cookies
  - Information stored on your computer by the browser
- Used for tracking, personalization, session management
  - Not executable, not generally a security risk
  - Unless someone gets access to them
- Could be considered be a privacy risk
  - Lots of personal data in there
- Session IDs are often stored in the cookie
  - Maintains sessions across multiple browser sessions

Header manipulation
- Information gathering
  - Wireshark, Kismet
- Exploits
  - Cross-site scripting
- Modify headers
  - Tamper, Firesheep, Scapy
- Modify cookies
  - Cookies Manager+ (Firefox add-on)

Prevent session hijacking
- Encrypt end-to-end
  - They can't capture your session ID if they can't see it
  - Additional load on the web server (HTTPS)
  - Firefox extension: HTTPS Everywhere, Force-TLS
- Encrypt end-to-somewhere
  - At least avoid capture over a local wireless network
  - Still in-the-clear for part of the journey
  - Personal VPN (OpenVPN, VyprVPN, etc.)
- Use session ID monitors
  - Blacksheep
  - Application-specific



1.2 - Driver Manipulation

Malware hide-and-go seek
- Traditional anti-virus is very good at identifying known attacks
  - Checks the signature
  - Block anything that matches
- There are still ways to infect and hide
  - It's a constant war
  - Zero-day attacks, new attack types, etc.

Your drivers are powerful
- The interaction between the hardware and your operating system
  - They are often trusted
  - Great opportunity for security issues
- May 2016 - HP Audio Drivers
  - Conexant audio chips
  - Driver installation includes audio control software
  - Debugging feature enables a keylogger
- Hardware interactions contain sensitive information
  - Video, keyboard, mouse

1.2 - Driver Manipulation (continued)

Shimming
- Filling in the space between two objects
  - A middleman
- Windows includes it's own shim
  - Backwards compatibility with previous Windows versions
  - Application Compatibility Shim Cache
- Malware authors write their own shims
  - Get around security (like UAC)
- January 2015 Microsoft vulnerability
  - Elevates privilege

Refactoring
- Metamorphic malware
  - A different program each time it's downloaded
- Make it appear different each time
  - Add NOP instructions
  - Loops, pointless code strings
- Can intelligently redesign itself
  - Reorder functions
  - Modify the application flow
  - Reorder code and insert unused data types
- Difficult to match with signature-based detection
  - Use a layered approach

1.2 - Spoofing

Spoofing
- Pretend to be something you aren't
  - Fake web server, fake DNS server, etc.
- Email address spoofing
  - The sending address of an email isn't really the sender
- Caller ID spoofing
  - The incoming call information is completely fake
- Man-in-the-middle attacks
  - The person in the middle of the conversation pretends to be both endpoints

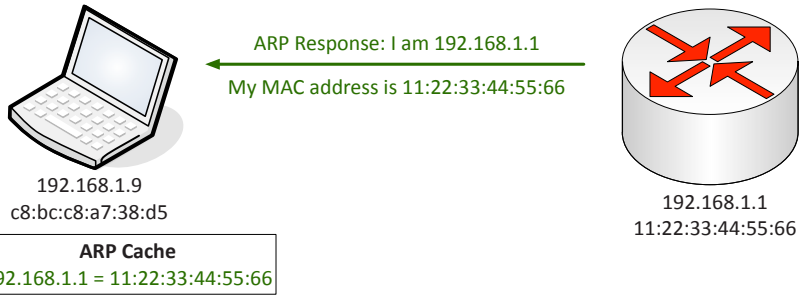
MAC spoofing
- Your Ethernet device has a MAC address
  - A unique burned-in address
  - Most drivers allow you to change this
- Changing the MAC address can be legitimate
  - Internet provider expects a certain MAC address
  - Certain applications require a particular MAC address
- It might not be legitimate
  - Circumvent MAC-based ACLs
  - Fake-out a wireless address filter
- Very difficult to detect
  - How do you know it's not the original device?

IP address spoofing
- Take someone else's IP address
  - Actual device
  - Pretend to be somewhere you are not
- Can be legitimate
  - Load balancing
  - Load testing
- May not be legitimate
  - ARP poisoning
  - DNS amplification / DDoS
- Easier to identify than MAC address spoofing
  - Apply rules to prevent invalid traffic, enable switch security

1

A legitimate response to an ARP request is received from the default gateway.

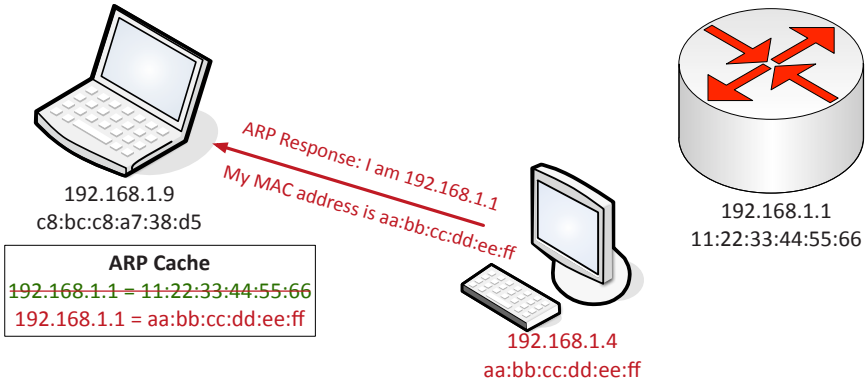
The ARP response is cached on the local device.



2

An attacker sends an ARP response that spoofs the IP address of the router and includes the attacker's MAC address.

The malicious ARP information replaces the cached record, completing the ARP poisoning.



1.2 - Wireless Replay Attacks

Wired vs. wireless replay

- Similar to a wired replay attacks
  - Wireless doesn't change those attacks
- Wireless adds some additional capabilities
  - This is a big concern for the security professional
- Much easier to capture the data
  - Hotspots are generally in the clear
  - Just like tuning in to a radio station

Cracking WEP

- WEP - Wired Equivalent Privacy
  - A broken security protocol
  - Could not stop the replay of 802.11 packets
- ARP request replay attack
  - Cracking WEP requires thousands of Initialization Vector (IV) packets
  - Wait all day to collect IV information
  - Or replay a ton of ARPs and collect the IV packets
- Now you have many thousands of IV packets
  - You can crack WEP in seconds

1.2 - Rogue Access Points and Evil Twins

Rogue Access Points

- A significant potential backdoor
  - Huge security concerns
- Very easy to plug in a wireless AP
  - Or enable wireless sharing in your OS
- Schedule a periodic survey
  - Walk around your building/campus
  - Use third-party tools / WiFi Pineapple
- Consider using 802.1X (Network Access Control)
  - You must authenticate, regardless of the connection type

Wireless Evil Twins

- Buy a wireless access point
  - -Less than $100 US
- Configure it exactly the same way as an existing network
  - -Same SSID and security settings
- Overpower the existing access points
  - -May not require the same physical location
- WiFi hotspots are easy to fool
  - -And they're wide open
- You encrypt your communication, right?
  - -Use HTTPS and a VPN

1.2 - Wireless Jamming

Radio frequency (RF) jamming

- Denial of Service
  - Prevent wireless communication
- Transmit interfering wireless signals
  - Decrease the signal-to-noise ratio at the receiving device
  - The receiving device can't hear the good signal
- Sometimes it's not intentional
  - Interference, not jamming
  - Microwave oven, fluorescent lights
- Jamming is intentional
  - Someone wants your network to not work

Wireless jamming

- Many different types
  - Constant, random bits / Constant, legitimate frames
- Data sent at random times
  - Random data and legitimate frames
- Reactive jamming
  - Only when someone else tries to communicate
- Needs to be somewhere close
  - Difficult to be effective from a distance
- Time to go fox hunting
  - You'll need the right equipment to hunt down the jam
  - Directional antenna, attenuator

1.2 - WPS Attacks

Using WPS

- Wi-Fi Protected Setup
  - Originally called Wi-Fi Simple Config
- Allows "easy" setup of a mobile device
  - A passphrase can be complicated to a novice
- Different ways to connect
  - PIN configured on access point must be entered on the mobile device
  - Or push a button on the access point
  - Near-field communication
    - Bring the mobile device close to the access point
  - USB method - no longer used

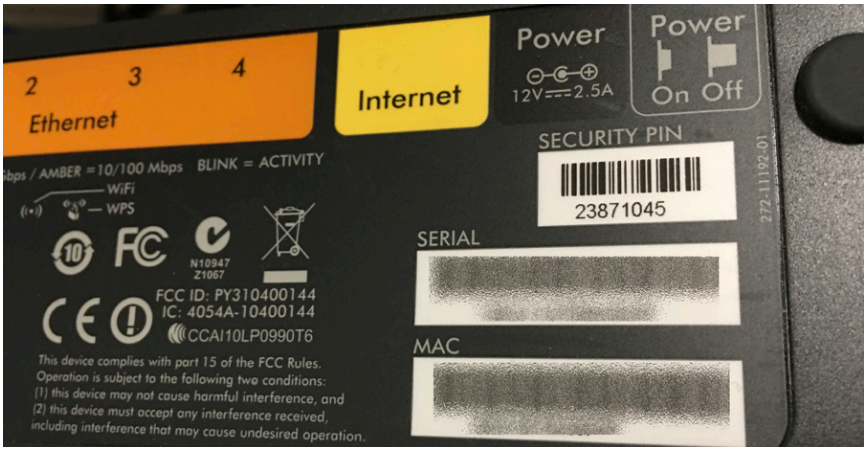
The WPS hack

- December 2011 - WPS has a design flaw
  - It was built wrong from the beginning
- PIN is an eight-digit number
  - Really seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities. Second half, 1,000 possibilities
- It used to take about four hours to go through all of them
  - Lockout and slowdown functions have now been implemented
  - Takes one day to one week

1.2 - WPS Attacks (continued)

Other WPS Attacks

- Walk up to the access point
  - Default PIN may be written on the device
  - Or just push the WPS button on the front
- Pixie Dust - Summer 2014
  - WPS PIN may be poorly encrypted
  - Based on the wireless chipset
  - Offline WPS brute force
  - Takes a few minutes or less
  - So much for slowdowns and lockouts
- WPS is just awful
  - Make sure it's disabled



1.2 - Bluejacking and Bluesnarfing

Bluejacking

- Sending of unsolicited messages to another device via Bluetooth
  - No mobile carrier required!
- Typical functional distance is about 10 meters
  - More or less, depending on antenna and interference
- Bluejack with an address book object
  - Instead of contact name, write a message
    - "You are Bluejacked!"
  - "You are Bluejacked! Add to contacts?"
- Third-party software may also be used
  - Blooover, Bluesniff

Bluesnarfing

- Access a Bluetooth-enabled device and transfer data
  - Contact list, calendar, email, pictures, video, etc.
- First major security weakness in Bluetooth
  - Marcel Holtmann in September 2003 and Adam Laurie in November 2003
  - This weakness was patched
- Serious security issue
  - If you know the file, you can download it without authentication

1.2 - RFID and NFC Attacks

RFID (Radio-frequency identification)

- It's everywhere
  - Access badges
  - Inventory/Assembly line tracking
  - Pet/Animal identification
  - Anything that needs to be tracked
- Radar technology
  - Radio energy transmitted to the tag
  - RF powers the tag, ID is transmitted back
  - Bidirectional communication
  - Some tag formats can be active/powered

RFID Attacks

- Data capture
  - View communication
  - Replay attack
- Spoof the reader
  - Write your own data to the tag
- Denial of service
  - Signal jamming
- Decrypt communication
  - Many default keys are on The Google

Near field communication (NFC)

- Two-way wireless communication
  - Builds on RFID, which was one-way
- Payment systems
  - Google wallet and MasterCard partnership
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

NFC Security Concern

- Remote capture
  - It's a wireless network
  - 10 meters for active devices
- Frequency jamming
  - Denial of service
- Relay / Replay attack
  - Man in the middle
- Loss of RFC device control
  - Stolen/lost phone

1.2 - Wireless Disassociation Attacks

It started as a normal day

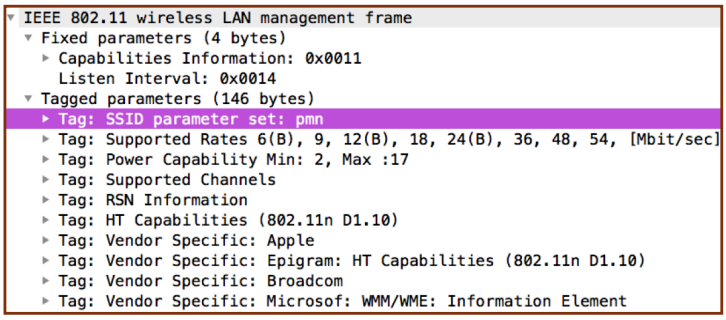
- Surfing along on your wireless network
  - And then you're not
- And then it happens again
  - And again
- You may not be able to stop it
  - There's (almost) nothing you can do
  - Time to get a long patch cable
- Wireless disassociation
  - A significant wireless denial of service (DoS) attack

802.11 management frames

- 802.11 wireless includes a number of management features
  - Frames that make everything work
  - You never see them
- Important for the operation of 802.11 wireless
  - How to find access points, manage QoS, associate/disassociate with an access point, etc.
- Original wireless standards did not add protection for management frames
  - Sent in the clear
  - No authentication or validation

Protecting against disassociation

- IEEE has already addressed the problem
  - 802.11w - July 2014
- Some of the important management frames are encrypted
  - Disassociate, deauthenticate, channel switch announcements, etc.
- Not everything is encrypted
  - Beacons, probes, authentication, association
  - Cart before the horse
- 802.11w is required for 802.11ac compliance
  - This will roll out going forward



1.2 - Cryptographic Attacks

Cryptographic attacks

- You've encrypted data and sent it to another person
  - Is it really secure?
  - How do you know?
- The bad guy doesn't have the combination (the key)
  - So they break the safe (the cryptography)
- Finding ways to undo the security
  - There are many potential cryptographic shortcomings

Birthday attack

- In a classroom of 23 students, what is the chance of two students sharing a birthday?
  - 23 students - about 50%
  - For a class of 30, the chance is about 70%
- In the digital world, this is a hash collision
  - A hash collision is the same hash value for two different plaintexts
  - Find a collision through brute force
- The attacker will generate multiple versions of plaintext to match the hashes
  - Protect yourself with a large hash output size

Known plaintext attack (KPA)

- Attacker has both the plaintext and the encrypted data
  - If you know the original plaintext, you may be able to find a "wedge" that is revealed in the ciphertext
  - The known plaintext is the crib
- WWII Enigma cipher
  - Easier to break if you knew some plaintext
  - Daily weather report (wetter)
  - Numbers were common (eins)
  - Royal Air Force would "seed" the North Sea with mines
  - Future messages would reference the harbor name

Rainbow tables

- An optimized, pre-built set of hashes
  - Doesn't need to contain every hash
  - The calculations have already been done
- Remarkable speed increase
  - Especially with longer password lengths
- Need different tables for different hashing methods
  - Windows is different than MySQL
- Rainbow tables won't work with salted hashes
  - Additional random value added to the original hash

Dictionary attacks

- People use common words as passwords
  - You can find them in the dictionary
- If you're using brute force, you should start with the easy ones
  - password, ninja, football
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- This will catch the low-hanging fruit
  - You'll need some smarter attacks for the smarter people

1.2 - Cryptographic Attacks (continued)

Brute force

- The password is the key
  - Secret phrase
  - Stored hash
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

The password file

- Different across operating systems
  - Different hash methods

Linux Account Hashes

```
Jumper Bay:1001::42e2f19c31c9ff73cb97eb1b26c10f54:::
Carter:1007::cf4eb977a6859c76efd21f5094ecf77d:::
Jackson:1008::e1f757d9cdc06690509e04b5446317d2:::
O'Neill:1009::78a8c423faedd2f002c6aef69a0ac1af:::
Teal'c:1010::bf84666c81974686e50d300bc36aea01:::
```

Collisions

- Hash digests are supposed to be unique
  - Different input data should never create the same hash
- MD5 hash
  - Message Digest Algorithm 5
  - First published in April 1992
  - Collisions identified in 1996
- December 2008: Researchers created CA certificate that appeared legitimate when MD5 is checked
  - Built other certificates that appeared to be legit and issued by RapidSSL

Downgrade attack

- Instead of using perfectly good encryption, use something that's not so great
  - Force the systems to downgrade their security
- 1995 - SSL/TLS vulnerability - FREAK - Factoring RSA Export Keys
  - Public key pairs can be limited to 512 bits or less
    - 1990 U.S. cryptography export regulations
  - Weak keys could be forced during the SSL handshake
  - Modern systems can easily brute force the small keys
  - Vulnerability was patched

Replay attacks

- Some cryptographic algorithms are more susceptible than others to a replay attack
  - A hash with no salt, no session ID tracking, no encryption
- Replay countermeasure may be part of the cryptography
  - Kerberos and Kerberos derivatives include time stamps
  - Anything after the time to live (TTL) is discarded

Weak implementations

- Weak encryption
  - One weak link breaks the entire chain
- 802.11 WEP
  - The RC4 key can be recovered by gathering enough packets
  - The algorithm didn't sufficiently protect the key
- DES - Data Encryption Standard
  - Relatively small 56-bit keys
  - Modern systems can brute force this pretty quickly

1.3 - Threat Actors

Threat actors and attributes

- The entity responsible for an event that has an impact on the safety of another entity
  - Also called a malicious actor
- Broad scope of actors
  - And motivations vary widely
- Intelligence can come from everywhere
  - Open source intelligence is a massive starting point

Script kiddies

- Runs premade scripts without any knowledge of what's really happening
  - Not necessarily a youngster
- Can be internal or external
  - But usually external
- Not very sophisticated
- No formal funding
  - Looking for low hanging fruit
- Motivated by the hunt
  - Working the ego, trying to make a name

Hacktivist

- A hacker with a purpose
  - Social change or a political agenda
  - Often an external entity
- Can be remarkably sophisticated
  - Very specific hacks
  - DoS, web site defacing, release of private documents, etc.
- Funding is limited
  - Some organizations have fundraising options

1.3 - Threat Actors (continued)

Organized crime
- Professional criminals
  - Motivated by money
  - Almost always an external entity
- Very sophisticated
  - Best hacking money can buy
- Crime that's organized
  - One person hacks, one person manages the exploits, another person sells the data, another handles customer support
- Lots of capital to fund hacking efforts

Nation states / APT
- Governments
  - National security, job security
  - Always an external entity
- Highest sophistication
  - Military control, utilities, financial control
  - United States and Israel destroyed 1,000 nuclear centrifuges with the Stuxnet worm
- Constant attacks
  - Advanced Persistent Threat (APT)
- Massive resources available

Insiders
- More than just passwords on sticky notes
  - Some insiders are out for no good
- Sophistication may not be advanced, but the insider has institutional knowledge
  - Attacks can be directed at vulnerable systems
  - The bad guy knows what to hit
- Extensive resources
  - Eating away from the inside

Competitors
- Many different motivations
  - DoS, espionage, harm reputation
- High level of sophistication
  - The competitive upside is huge (and very unethical)
- Many different intents
  - Shut down your competitor during an event
  - Steal customer lists
  - Corrupt manufacturing databases
  - Take financial information

1.4 - Penetration Testing

Penetration Testing
- Pentest
  - Simulate an attack
- Similar to vulnerability scanning
  - Except we actually try to exploit the vulnerabilities
- Often a compliance mandate
  - Regular penetration testing by a 3rd-party
- Technical Guide to Information Security Testing and Assessment
  - http://www.professormesser.link/800115

Verify a threat exists
- Stay up-to-date
  - New threats all the time
- National Institute of Standards and Technology National Vulnerability Database
  - http://nvd.nist.gov
- Perform regular vulnerability scans
  - Update your signatures
- Watch the news - Copycats are prevalent

Passive reconnaissance
- Learn as much as you can from open sources
  - There's a lot of information out there
  - Remarkably difficult to protect or identify
- Social media
- Corporate web site, online forums, Reddit
- Social engineering, dumpster diving
- Business organizations

Active reconnaissance
- Trying the doors
  - Maybe one is unlocked
  - Don't open it yet
  - Relatively easy to be seen
- Ping scans, port scans
- DNS queries
- OS scans, OS fingerprinting
- Service scans, version scans

Exploiting vulnerabilities
- Try to break into the system
  - Be careful; this can cause a denial of service or loss of data
  - Buffer overflows can cause instability
  - Gain privilege escalation
- You may need to try many different vulnerability types
  - Password brute-force
  - Social engineering
  - Database injections
  - Buffer overflows
- You'll only be sure you're vulnerable if you can bypass security
  - If you can get through, the bad guys can get through

1.4 - Penetration Testing (continued)

The process

- Initial exploitation
  - Get into the network
  - A challenging hurdle (most of the time)
- Persistence
  - Once you're there, you need to make sure there's a way back in
  - Set up a backdoor
  - Build user accounts, change or verify default passwords
- The pivot
  - The foothold point
  - The inside of the network is often relatively open
  - Jump from here to the rest of the network

Black box, white box, and grey box

- How much do you know about the test?
  - Many different approaches
- Black box / Unknown environment
  - The pentester knows nothing about the systems under attack
  - "Blind" test
- White box / Known environment
  - Full disclosure
- Grey box / Partially known environment
  - A mix of black and white
  - Focus on certain systems or applications

1.5 - Vulnerability Scanning

Vulnerability scanning

- Usually minimally invasive, unlike a penetration test
- Port scan - Poke around and see what's open
- Identify systems and security devices
- Test from the outside and inside
  - Don't dismiss insider threats
- Gather as much information as possible
  - We'll separate wheat from chaff later

Scan types

- Scanners are very powerful
  - Use many different techniques to identify vulnerabilities
- Non-intrusive scans
  - Gather information, don't try to exploit a vulnerability
- Intrusive scans
  - You'll try out the vulnerability to see if it works
- Non-credentialed scans
  - The scanner can't login to the remote device
- Credentialed scan
  - You're a normal user, emulates an insider attack

Identify vulnerability

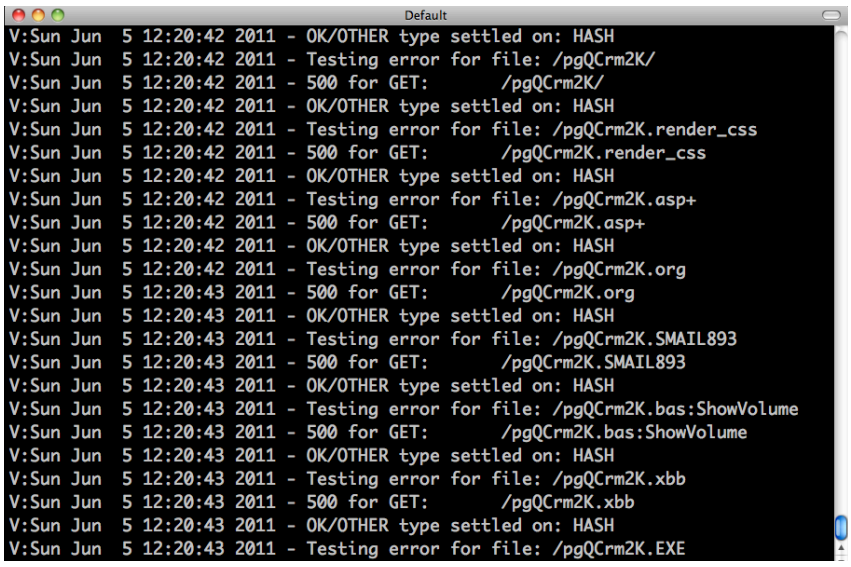
- The scanner looks for everything
  - Well, not _everything_
  - The signatures are the key
- The vulnerabilities can be cross-referenced online
  - Almost all scanners give you a place to go
  - National Vulnerability Database: http://nvd.nist.gov/
  - Microsoft Security Bulletins
- Some vulnerabilities cannot be definitively identified
  - You'll have to check manually to see if a system is vulnerable
  - But the scanner gives you a heads-up

Vulnerability scan results

- Lack of security controls
  - No firewall, no anti-virus, no anti-spyware
- Misconfigurations - Open shares, guest access
- Real vulnerabilities
  - Especially newer ones, occasionally the old ones

Dealing with false positives

- False positives
  - A vulnerability is identified that doesn't really exist
- This is different than a low-severity vulnerability
  - It's real, but it may not be your highest priority
- False negatives
  - A vulnerability exists, but you didn't detect it
- Update to the latest signatures
  - If you don't know about it, you can't see it
  - Work with the vulnerability detection manufacturer
  - They may need to update their signatures for your environment



1.6 - Vulnerability Types

Vulnerability types
- There are many types of vulnerabilities
  - Some digital, some physical
- Cover a broad scope
  - Programming, network design, process/procedure
- Any of these can be exploited at any time
  - Or multiples at the same time
  - Be on your toes

Race condition
- A programming conundrum
  - Sometimes, things happen at the same time
  - This can be bad if you've not planned for it
- Two bank accounts with $100
  - User 1 and User 2 transfer $50 from Account A to Account B
  - Expected outcome: Account A has $50, Account B has $150
- What if you don't perform proper validation?
  - User 1 and User 2 check the account balances ($100 in each account)
  - User 1 transfers $50 from Account A (now at $50) to Account B (now at $150)
  - At about the same time, user 2 transfers $50 from Account A (still has $100, right?, so now at $50) to Account B (now at $200)
  - Outcome: Account A has $50, Account B has $200

Race conditions can cause big problems
- January 2004 - Mars rover "Spirit"
  - Reboot when a problem is identified
  - Problem is with the file system and prevents rebooting
  - Reboot because of the file system problem
- GE Energy - Energy Management System
  - When multiple power lines failed at the same time, no alert was sent
  - Caused the Northeast Blackout of 2003
- Therac-25 radiation therapy machine in the 1980s
  - Used software interlocks instead of hardware
  - Race condition caused 100 times the normal dose of radiation
  - Six patients injured, three deaths

End-of-life vulnerabilities
- End-of-life
  - Without vendor support, no security patches
- March 2017 - Microsoft patches Windows to protect against SMB vulnerability
  - Windows XP, Windows 8, and Server 2003 were end-of-life and not included
- May 2017 - WannaCrypt ransomware infects hundreds of thousands of computers
  - End-of-life systems were wide open
- Upgrade to maintain security
  - No other choice

Embedded system vulnerabilities
- No direct access to the operating system
  - You'll probably never see it
- These devices are usually connected to the Internet
  - Very convenient to the hacker
- Old, outdated operating system software
  - Why upgrade? May not even be upgradable.
- June 2017 - Wikileaks releases CIA files called Vault7
  - CIA takes advantage of vulnerabilities on Linksys and D-Link routers
  - They can easily get your administrative password
  - At which point they install their own firmware

Lack of vendor support
- Security requires diligence
  - The potential for a vulnerability is always there
- Vendors are the only ones who can fix their products
  - Assuming they know about the problem
  - And care about fixing it
- Trane Comfortlink II thermostats
  - Control the temperature from your phone
  - Trane notified of three vulnerabilities in April 2014
  - Two patched in April 2015, one in January 2016

Improper input handling
- Many applications accept user input
  - We put data in, we get data back
- All input should be considered malicious
  - Check everything. Trust nobody.
- Allowing invalid input can be devastating
  - SQL injections, buffer overflows, denial of service
- It takes a lot of work to find input that can be used maliciously
  - But they will find it

Improper error handling
- Errors happen
  - And you should probably know about it
- Messages should be just informational enough
  - Avoid too much detail
  - Network information, memory dump, stack traces, database dumps
- This is an easy one to find and fix
  - A development best-practice

Misconfiguration/weak configuration
- Very easy to leave a door open
  - The hackers will always find it
- September 2015 - Patreon is compromised
  - Used a debugger to help troubleshoot site issues
  - Was left exposed to the Internet
  - Effectively allowed for remote code executions
  - Gigabytes of customer data was released online
- June 2017 - 14 million Verizon records exposed
  - Third-party left an Amazon S3 data repository open
  - Researcher found the data before the bad guys

1.6 - Vulnerability Types (continued)

Default configuration
- Every application and network device has a default login
  - Not all of these are ever changed
- Mirai botnet
  - Takes advantage of default configurations
  - Takes over Internet of Things (IoT) devices
  - 60+ default configurations
  - Cameras, routers, doorbells, garage door openers, etc.
- Mirai released as open-source software

Untrained users
- It takes one person to allow a breach
  - And it can happen without the user even knowing
- Training is critical
  - Emails don't work
  - This is time consuming and expensive (and important)
- Annual reinforcement
  - Quiz and role play
  - Become familiar with common situations

Improperly configured accounts
- Technical issue and process issue
  - Frequent audits are important
- Accounts without a need
  - Abandoned and unnecessary accounts
- Accounts with administrative access
  - These should be severely limited
- Should not be able to login directly as administrator
  - Unless it's on a server console

Vulnerable business processes
- If there's a way to game the system, the bad guys will find it
  - It doesn't have to be a technical vulnerability
- The Society for Worldwide Interbank Financial Telecommunication (SWIFT)
  - Electronically send payment instructions between banks
- February 2016 - Bangladesh Bank
  - Dridex malware used to steal SWIFT credentials
  - Attempted to steal $951 million while the bank was closed
  - Hackers misspelled "Foundation" as "Fundation"
  - $81 million was lost

Weak cipher suites
- The suite
  - Encryption protocol (AES, 3DES, etc.)
  - Encryption key length (40 bits, 128 bits, 256 bits, etc.)
  - Hash used for the integrity check (SHA, MD5, etc.)
- Some cipher suites are easier to break than others
  - Stay updated with the latest best practices
- TLS is one of the most common issues
  - Over 300 cipher suites
- Which are good and which are bad?
  - Weak or null encryption (less than 128 bit key sizes), outdated hashes (MD5)

Memory/buffer vulnerabilities
- Manipulating memory can be advantageous
  - Relatively difficult to accomplish
- Memory leak
  - Unused memory is not properly released
  - Begins to slowly grow in size
  - Eventually uses all available memory
  - System crashes
- Integer overflow
  - Large number into a smaller sized space
  - Where does the extra number go?
  - You shouldn't be able to manipulate memory this way
- Buffer overflow
  - Overwriting a buffer of memory
  - Spills over into other memory areas
- NULL Pointer dereference
  - Programming technique that references a portion of memory
  - What happens if that reference points to nothing?
  - Application crash, debug information displayed, Denial of Service, etc.
- DLL injection
  - The bad guys didn't write the application
  - But they could write an external library and manipulate the operating system or application to run the library

System sprawl/undocumented assets
- Hundreds of projects, test platforms, active operating systems, production VMs
  - Spin up a new instance with a click
  - Keeping track is a challenge
- Easy to miss a forgotten computer
  - Under a desk
  - Part of a retired application
- Not part of regular security patches
  - These become pivot points

Architecture/design weaknesses
- The best security system fails if you don't have locks on the doors
  - The network doors aren't always visible
- Examine every part of the network
  - Ingress
  - VPN
  - Third-party access
  - Internal controls
  - Account access
  - Front door access
  - Conference room access

1.6 - Vulnerability Types (continued)

New threats/zero day

- What you don't know can really hurt you
  - And you won't even see it coming
- Vulnerabilities are sitting in your system, waiting for someone to find them
  - Some problems are hidden for years
- As soon as the problem is discovered (day zero), patch it
  - There isn't always time to properly test
  - Balance severity with stability
- WannaCry ransomware hit on May 12, 2017
  - However, the patch had been available since March 14

Improper certificate and key management

- Manage your keys and certificates
  - This needs to be well planned
  - Important decisions, can't do this on the fly
- What will be the organization's certificate authority?
- How will the CA content be protected?
- How will intermediate CAs be created and managed?
- Who will validate and sign the organization's certificates?
- What is the validation process?
- And many more

2.1 - Firewalls

The universal security control

- Standard issue
  - Home, office, and in your operating system
- Control the flow of network traffic
  - Everything passes through the firewall
- Corporate control of outbound and inbound data
  - Sensitive materials
- Control of inappropriate content
  - Not safe for work, parental controls
- Protection against evil - Anti-virus, anti-malware

Network based firewalls

- Filters traffic by port number
  - OSI layer 4 (TCP/UDP)
  - Some firewalls can filter through OSI layer 7
- Can encrypt traffic into/out of the network
  - Protect your traffic between sites
- Can proxy traffic
  - A common security technique
- Most firewalls can be layer 3 devices (routers)
  - Usually sits on the ingress/egress of the network

Stateless firewall

- Does not keep track of traffic flows
  - Each packet is individually examined, regardless of past history
  - Traffic sent outside of an active session will traverse a stateless firewall

Stateful firewall

- Stateful firewalls remember the "state" of the session
  - Everything within a valid flow is allowed

Application-aware security devices

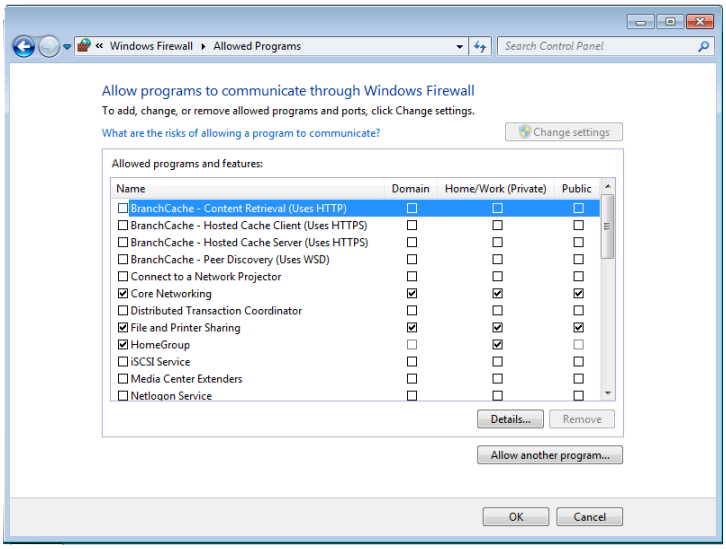
- The OSI Application Layer
  - All data in every packet
- Can be called different names
  - Application layer gateway
  - Stateful multilayer inspection
  - Deep packet inspection
- Requires some advanced decodes
  - Every packet must be analyzed and categorized before a security decision is determined

Application-aware security devices

- Network-based Firewalls
  - Control traffic flows based on the application
  - Microsoft SQL Server, Twitter, YouTube
- Intrusion Prevention Systems
  - Identify the application
  - Apply application-specific vulnerability signatures to the traffic
- Host-based firewalls
  - Work with the OS to determine the application

Firewall rules

- Access control lists (ACLs)
  - Allow or disallow traffic based on tuples
  - Groupings of categories
  - Source IP, Destination IP, port number, time of day, application, etc.
- A logical path
  - Usually top-to-bottom
- Can be very general or very specific
  - Specific rules are usually at the top
- Implicit deny
  - Most firewalls include a deny at the bottom
  - Even if you didn't put one



2.1 - VPN Concentrators

VPN Concentrator
- Virtual Private Network
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

Remote access VPN
- On-demand access from a remote device
  - Software connects to a VPN concentrator
- Some software can be configured as always-on

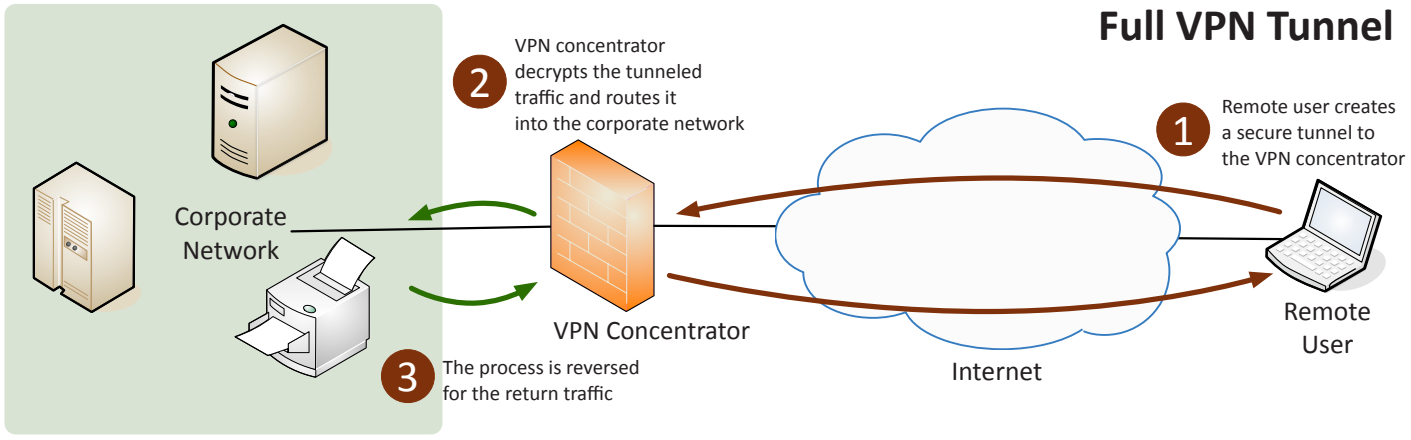
SSL VPN (Secure Sockets Layer VPN)
- Uses common SSL/TLS protocol (tcp/443)
  - (Almost) No firewall issues!
- No big VPN clients
  - Usually remote access communication
- Authenticate users
  - No requirement for digital certificates or shared passwords (like IPSec)
- Can be run from a browser or from a VPN client
  - Across many operating systems

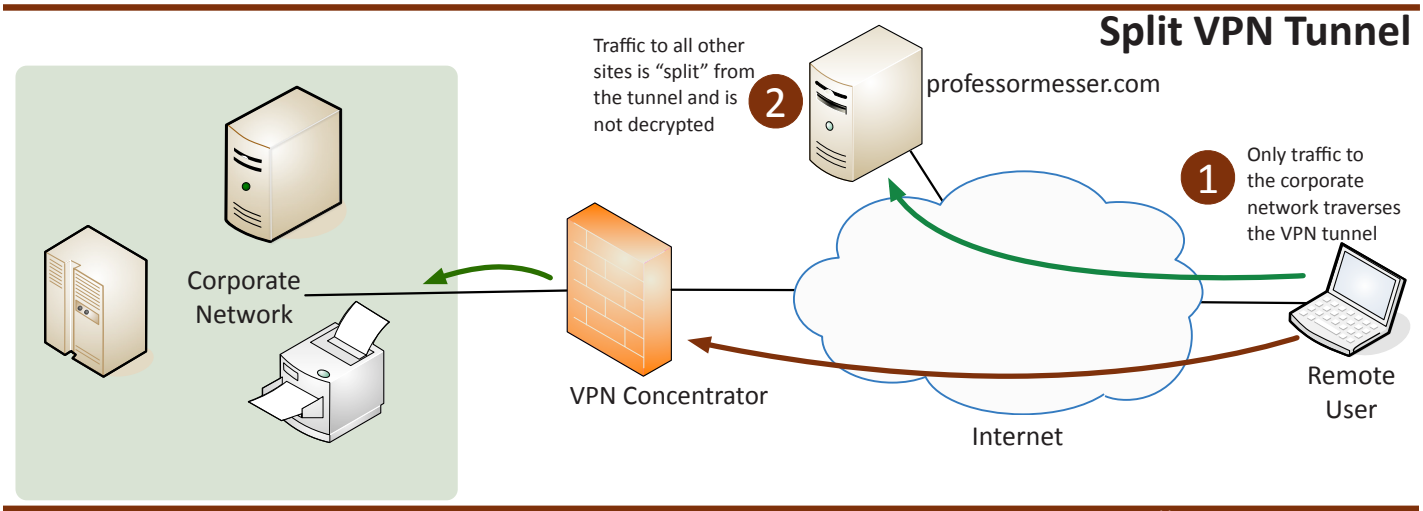
Site-to-site VPN
- Always-on
  - Or almost always
- Firewalls often act as VPN concentrators
  - Probably already have firewalls in place

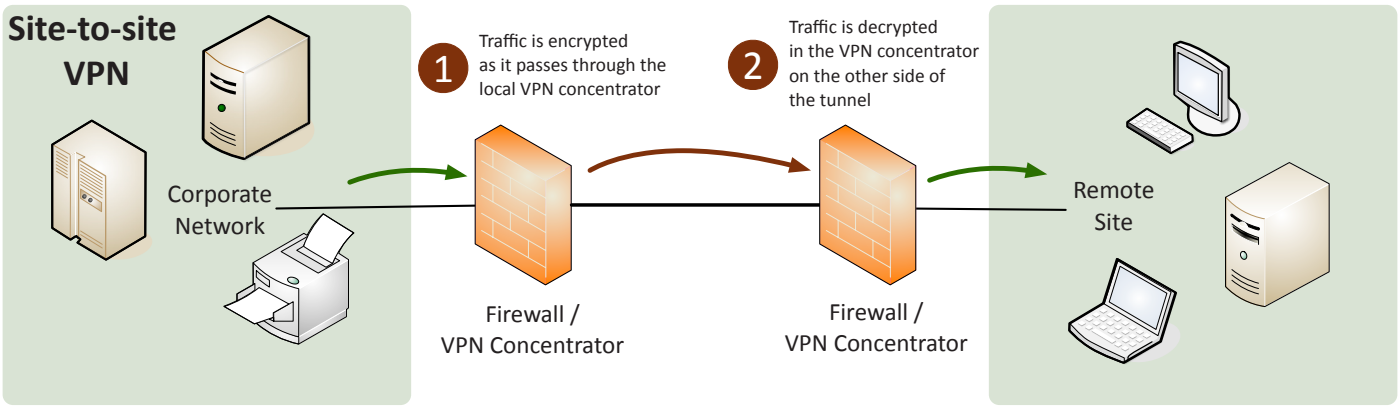
IP Sec (Internet Protocol Security)
- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)

Authentication Header
- Hash of the packet and a shared key
  - MD5, SHA-1, or SHA-2 are common
  - Adds the AH to the packet header

Encapsulation Security Payload (ESP)
- Encrypts the packet
  - MD5, SHA-1, or SHA-2 for hash, and 3DES or AES for encryption
  - Adds a header, a trailer, and an Integrity Check Value

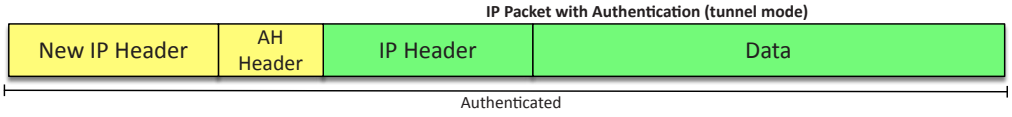






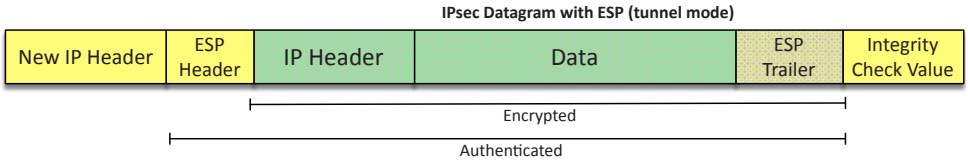
AH (Authentication Header)

- Data integrity
- Origin authentication
- Replay attack protection
- Keyed-hash mechanism
- No confidentiality/encryption



ESP (Encapsulating Security Payload)

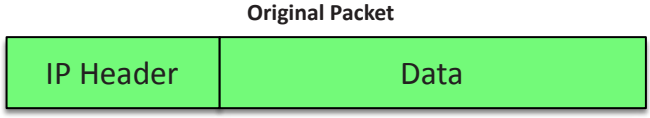
- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Anti-replay protection

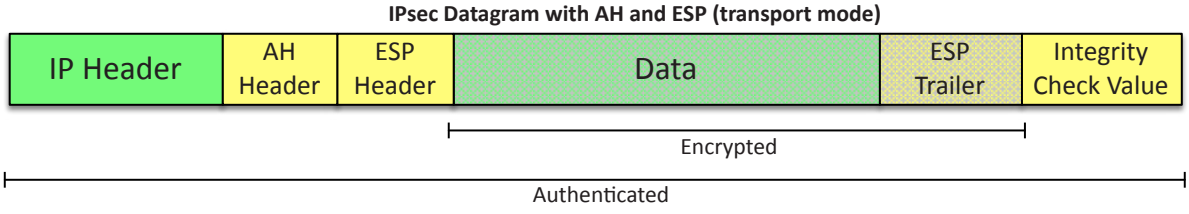


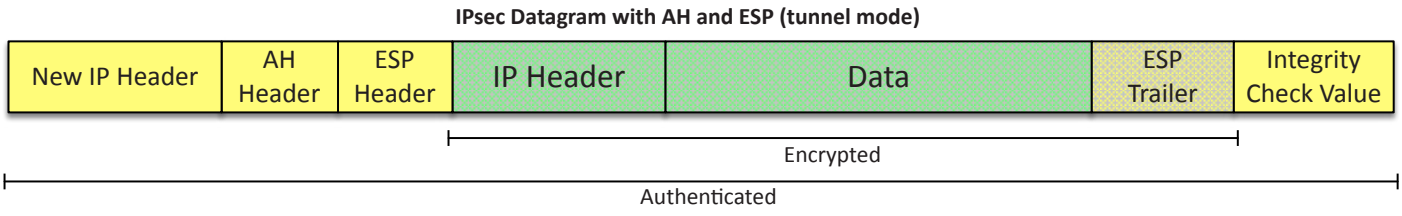
IPsec Transport mode and Tunnel mode

AH and ESP

- Combine the data integrity of AH with the confidentiality of ESP







2.1 - Network Intrusion Detection and Prevention

NIDS and NIPS
- Intrusion Detection System / Intrusion Prevention System
  - Watch network traffic
- Intrusions
  - Exploits against operating systems, applications, etc.
  - Buffer overflows, cross-site scripting, other vulnerabilities
- Detection vs. Prevention
  - Detection – Alarm or alert
  - Prevention – Stop it before it gets into the network

Passive monitoring
- Examine a copy of the traffic
  - Port mirror (SPAN), network tap
- No way to block (prevent) traffic

Out-of-band response
- When malicious traffic is identified, IPS sends TCP RST (reset) frames
  - After-the-fact
  - Limited UDP response available

Inline monitoring
- IDS/IPS sits physically inline
  - All traffic passes through the IDS/IPS

In-band response
- Malicious traffic is immediately identified
  - Dropped at the IPS
  - Does not proceed through the network

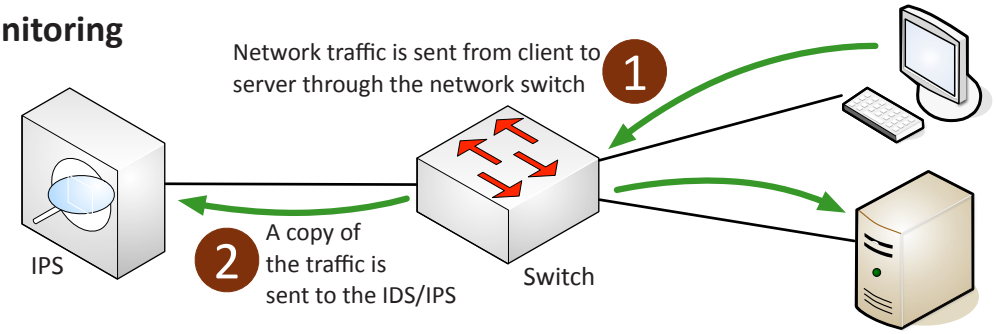
Identification technologies
- Signature-based - Look for a perfect match
- Anomaly-based - Build a baseline of what's "normal"
- Behavior-based - Observe and report
- Heuristics - Use artificial intelligence to identify

IPS Rules
- You determine what happens with unwanted traffic
  - Block, allow, send an alert, etc.
- Thousands of rules
  - Or more
- Rules can be customized by group
  - Or as individual rules
- This can take time to find the right balance
  - Security / alert "noise" / false positives

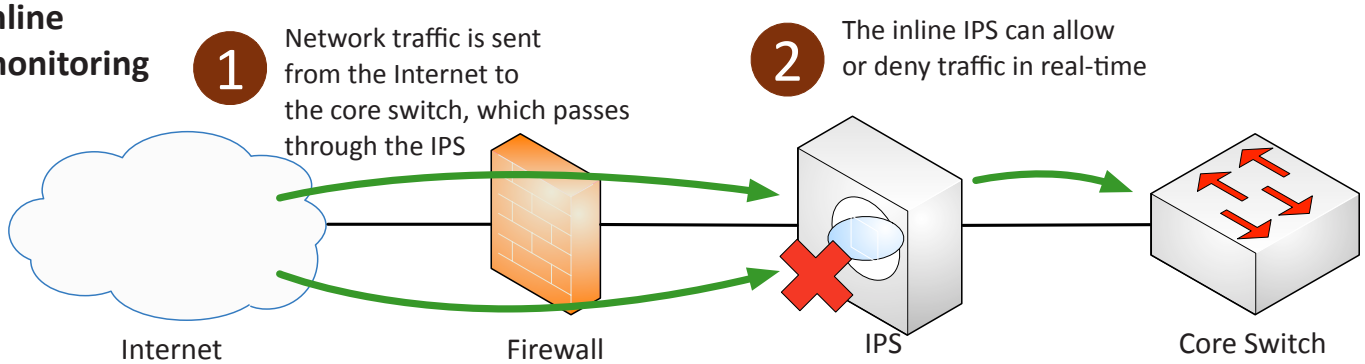
False Positives
- A report that isn't true
  - A false alarm or mistaken identity
- IDS/IPS information
  - Only as good as the signatures
  - Some legitimate traffic could be marked as malicious
  - Time-consuming to research and resolve
- Workstation antivirus
  - April 2017: Webroot Antivirus
  - Windows files quarantined as malicious
  - Facebook and Bloomberg marked as phishing sites
- Consider a second opinion
  - http://www.VirusTotal.com

False Negatives
- A report missed identifying something
  - You didn't get a notification
- Malicious traffic got through your defenses
  - You'll probably see the results of this
- It's difficult to know when this happens
  - It's completely silent
- Get catch/miss rates with industry tests
  - IPS, anti-virus

Passive monitoring



Inline monitoring



2.1 - Router and Switch Security

Routers
- Routes traffic between IP subnets
  - OSI layer 3 device
  - Routers inside of switches sometimes called "layer 3 switches"
- Layer 2 = Switch, Layer 3 = Router
- Often connects diverse network types
  - LAN, WAN, copper, fiber

Access Control Lists (ACLs)
- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Incoming or outgoing
- ACLs evaluate on certain criteria
  - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?
- ACLs have evolved through the years
  - Standard vs. Extended, numbered vs. named

Anti-spoofing
- Prevent a bad guy from using someone else's address
  - Man-in-the-middle, DDoS, etc.
- Filter reserved IP addresses
  - An RFC 1918 address should not be routed to or from the Internet
  - A simple ACL will work
- Enable Reverse Path Forwarding (RPF)
  - The response to an inbound packet should return the same way
  - If it doesn't, then drop the packet right now

Switches
- Bridging done in hardware
  - Application-specific integrated circuit (ASIC)
- An OSI layer 2 device
  - Forwards traffic based on data link address
- Many (many) ports
  - The core of an enterprise network
- High bandwidth
  - Many simultaneous packets

Switch port security
- The inside of your network is relatively insecure
  - We often spend our time protecting against the outside
- Copper and wireless (and fiber)
  - It's all a conduit to your network
  - Wireless doesn't even have to be in the building
- It's often very easy to connect to the network
  - We want the conference rooms to be convenient

Network Access Control (NAC)
- IEEE 802.1X - Port-based Network Access Control (NAC)
  - You don't get access until you authenticate
  - Makes extensive use of EAP and RADIUS
  - Extensible Authentication Protocol / Remote Authentication Dial In User Service
- We're talking about physical interfaces
  - Not TCP or UDP ports
- Administrative enable/disable
  - Disable your unused ports
- Duplicate MAC address checking
  - Stop the spoofers

Loop Prevention
- Connect two switches to each other
  - They'll send traffic back and forth forever
  - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network
  - And somewhat difficult to troubleshoot
  - Relatively easy to resolve
- Spanning Tree Protocol
  - IEEE standard 802.1D to prevent loops in bridged (switched) networks (1990)
  - Created by Radia Perlman
  - Used practically everywhere

Flood Guard
- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Interface is usually disabled by default

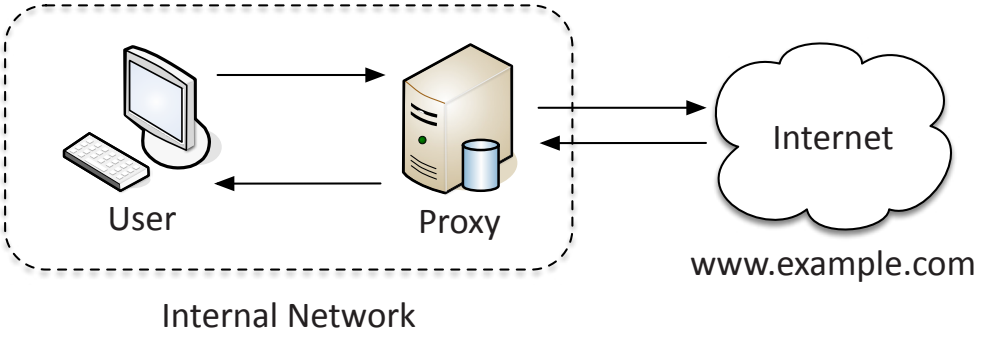
Layer 3 switches
- A switch (Layer 2) and router (Layer 3) in the same physical device
- Switching still operates at OSI Layer 2, routing still operates at OSI Layer 3
  - There's nothing new or special happening here

2.1 - Proxies

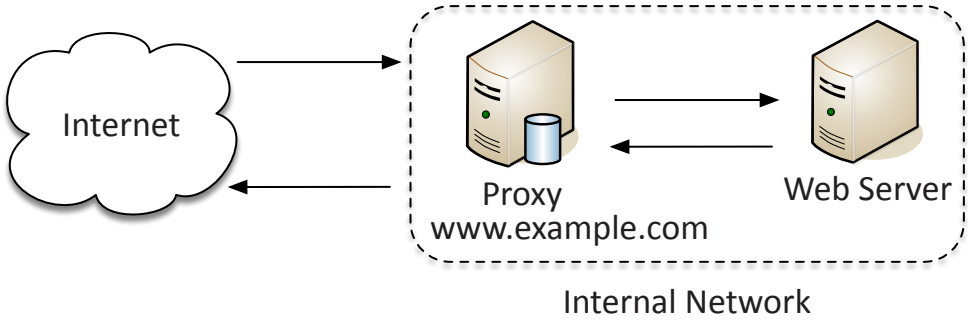
Proxies
- Sits between the users and the external network
- Receives the user requests and sends the request on their behalf (the proxy)
- Useful for caching information, access control, URL filtering, content scanning
- Applications may need to know how to use the proxy (explicit)
- Some proxies are invisible (transparent)

Application proxies
- One of the simplest "proxies" is NAT
  - A network-level proxy
- Most proxies in use are application proxies
  - The proxy understands the way the application works
- A proxy may only know one application
  - HTTP
- Many proxies are multipurpose proxies
  - HTTP, HTTPS, FTP, etc.

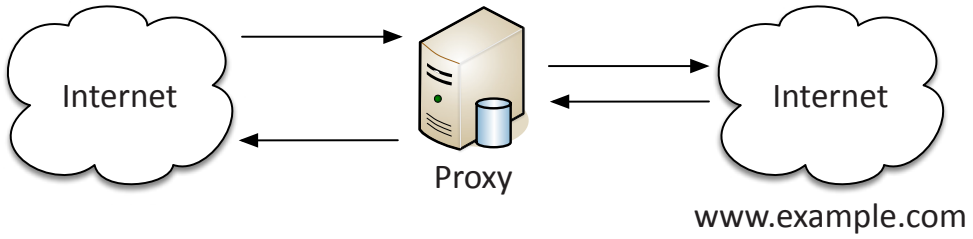
Forward Proxy
- An "internal proxy"
  - Commonly used to protect and control user access to the Internet



Reverse Proxy
- Inbound traffic from the Internet to your internal service

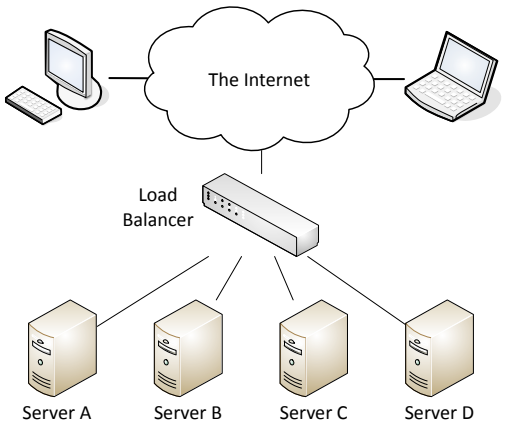


Open Proxy
- A third-party, uncontrolled proxy
  - Can be a significant security concern
  - Often used to circumvent existing security controls



2.1 - Load Balancers

Balancing the Load
- Distribute the load
  - Multiple servers
  - Invisible to the end-user
- Large-scale implementations
  - Web server farms, database farms
- Fault tolerance
  - Very fast convergence



Load Balancer
- Configurable load
  - Manage across servers
- TCP offload
  - Protocol overhead
- SSL offload
  - Encryption/Decryption
- Caching - Fast response
- Prioritization - QoS
- Content switching
  - Application-centric balancing

2.1 - Load Balancers (continued)

Scheduling
- Round-robin
  - Each server is selected in turn
- Weighted round-robin
  - Prioritize the server use
- Dynamic round-robin
  - Monitor the server load and distributed to the server with the lowest use

Active/Active load balancing
- Affinity - A kinship, a likeness
- Many applications require communication to the same instance
  - Each user is “stuck” to the same server
  - Tracked through IP address or session IDs
  - Source affinity

Active/passive load balancing
- Some servers are active
  - Others are on standby
- If an active server fails, the passive server takes its place

2.1 - Access Points

Wireless Access Point (WAP)
- Not a wireless router
  - A wireless router is a router and a WAP in a single device
- WAP is a bridge
  - Extends the wired network onto the wireless network
  - WAP is an OSI layer 2 device

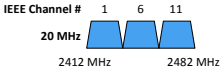
SSID management
- Service Set Identifier
  - Name of the wireless network
  - LINKSYS, DEFAULT, NETGEAR
- Change the SSID to something not-so obvious
- Disable SSID broadcasting?
  - SSID is easily determined through wireless network analysis
  - Security through obscurity

MAC filtering
- Media Access Control
  - The “hardware” address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity

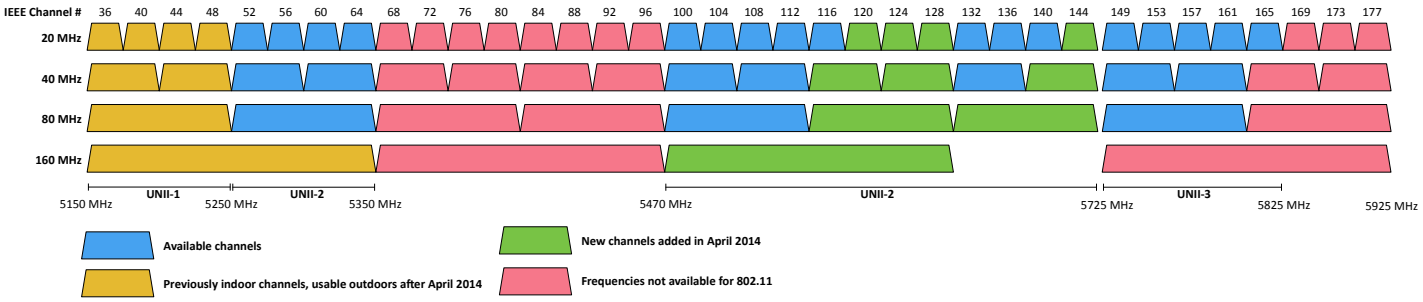
Power Level Controls
- Usually a wireless configuration
  - Set it as low as you can
- How low is low?
  - This might require some additional study
- Consider the receiver
  - High-gain antennas can hear a lot
  - Location, location, location

Band selection and bandwidth
- Throughput
  - Maximum theoretical throughputs
  - Actual throughput can vary widely
- Frequency
  - 2.4 GHz and 5 GHz
  - -And sometimes both
- Distance
  - A combination of antennas
- Channels
  - Non-overlapping channels would be ideal

2.4 GHz Spectrum for 802.11 - North America



5 GHz Spectrum for 802.11 - North America



2.1 - Access Points (continued)

Omnidirectional antennas
- One of the most common
  - Included on most access points
- Signal is evenly distributed on all sides
  - Omni=all
- Good choice for most environments
  - You need coverage in all directions
- No ability to focus the signal
  - A different antenna will be required

Directional antennas
- Focus the signal
  - Increased distances
- Send and receive in a single direction
  - Focused transmission and listening
- Antenna performance is measured in dB
  - Double power every 3dB of gain

Directional antennas
- Yagi antenna
  - Very directional and high gain
- Parabolic antenna
  - Focus the signal to a single point

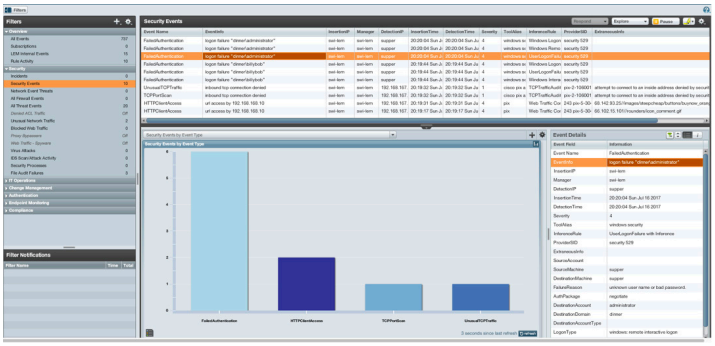
Managing wireless configurations
- LWAPP
  - Lightweight Access Point Protocol
  - Cisco proprietary - CAPWAP is an RFC standard, based on LWAPP
  - Manage multiple access points simultaneously
- Thick/fat access points
  - The access point handles most wireless tasks
  - The switch is not wireless-aware
- Thin access points
  - Just enough to be 802.11 wireless
  - The intelligence is in the switch
  - Less expensive

Wireless LAN controllers
- Centralized management of WAPs - A single “pane of glass”
- Deploy new access points
- Performance and security monitoring
- Configure and deploy changes to all sites
- Report on access point use
- Usually a proprietary system
  - The wireless controller is paired with the access points

2.1 - SIEM

SIEM
- Security Information and Event Management
  - Security events and information
- Security alerts - Real-time information
- Log aggregation and long-term storage
  - Usually includes advanced reporting features
- Data correlation - Link diverse data types
- Forensic analysis - Gather details after an event

Time Synchronization
- Switches, routers, firewalls, servers, workstations
  - Every device has its own clock
- Synchronizing the clocks becomes critical
  - Log files, authentication information, outage details
- Automatic update with NTP (Network Time Protocol)
  - No flashing 12:00 lights
- Flexible - You control how clocks are updated
- Very accurate
  - Accuracy is better than 1 millisecond on a local network



Syslog
- Standard for message logging
  - Diverse systems, consolidated log
- Usually a central logging receiver
  - Integrated into the SIEM
- You’re going to need a lot of disk space
  - No, more. More than that.
- WORM drive technology
  - Write Once Read Many
  - Protect important security logs

Event de-duplication
- Event storms
  - When it rains, it pours
- Filter out the noise
  - Focus on the real problems
- Flapping (down/up/down)
  - Timers used to suppress ongoing messages
- Configurable suppression
  - Define your own event handling
  - Useful for automating responses

Automated alerting and triggers
- Constant information flow
  - Important metrics in the incoming logs
- Track important statistics
  - Exceptions can be identified
- Send alerts when problems are found
  - Email, text, call, etc.
- Create triggers to automate responses
  - Open a ticket, reboot a server

2.1 - Data Loss Prevention

Data Loss Prevention (DLP)
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the bad guys get it - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions in different places

Data Loss Prevention (DLP) systems
- On your computer - Data in use, Endpoint DLP
- On your network - Data in motion
- On your server - Data at rest

USB Blocking
- DLP on a workstation - Allow or deny certain tasks
- November 2008 - U.S. Department of Defense
  - Worm virus "agent.btz" replicates using USB storage
  - Bans removable flash media and storage devices
- All devices had to be updated -
  - Local DLP agent handled USB blocking
- Ban was lifted in February 2010 - Replaced with strict guidelines

Cloud based DLP
- Located between users and the Internet
  - Watch every byte of network traffic
  - No hardware, no software
- Block custom defined data strings
  - Unique data for your organization
- Manage access to URLs - Prevent file transfers to cloud storage
- Block viruses and malware - Anything traversing the network

DLP and email
- Email continues to be the most critical risk vector
  - Inbound threats, outbound data loss
- Check every email inbound and outbound
  - Internal system or cloud-based
- Inbound
  - Block keywords, identify impostors, quarantine email messages
- Outbound
  - Fake wire transfers, W-2 transmissions, employee information

Emailing a spreadsheet template
- November 2017
- Boeing employee emails spouse a spreadsheet to use as a template
- Contained the personal information of 36,000 Boeing employees
  - In hidden columns
  - Social security numbers, date of birth, etc.
- Boeing sells its own DLP software
  - But only uses it for classified work

2.1 - Network Access Control

Edge vs. access control
- Control at the edge
  - Your Internet link
  - Managed primarily through firewall rules
  - Firewall rules rarely change
- Access control
  - Control from wherever you are
- Inside or outside
  - Access can be based on many rules
- By user, group, location, application, etc.
  - Access can be easily revoked or changed
- Change your security posture at any time

Posture assessment
- You can't trust everyone's computer
  - BYOD (Bring Your Own Device)
  - Malware infections / missing anti-malware
  - Unauthorized applications
- Before connecting to the network, perform a health check
  - Is it a trusted device?
  - Is it running anti-virus? Which one? Is it updated?
  - Are the corporate applications installed?
  - Is it a mobile device? Is the disk encrypted?
  - The type of device doesn't matter
  - Windows, Mac, Linux, iOS, Android

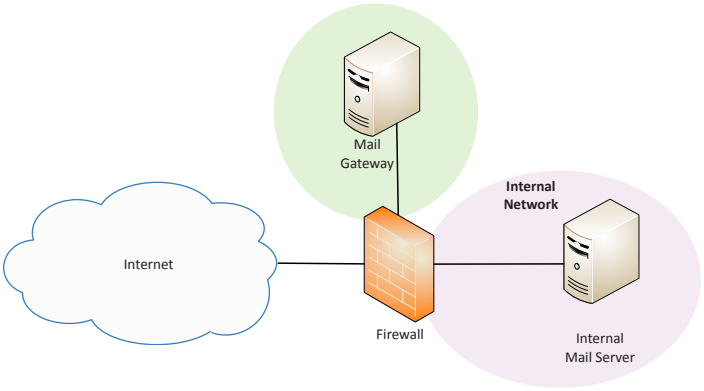
Health checks/posture assessment
- Persistent agents
  - Permanently installed onto a system
  - Periodic updates may be required
- Dissolvable agents
  - No installation is required
  - Runs during the posture assessment
  - Terminates when no longer required
- Agentless NAC
  - Integrated with Active Directory
  - Checks are made during login and logoff
  - Can't be scheduled

Failing assessment
- What happens when a posture assessment fails?
  - Too dangerous to allow access
- Quarantine network, notify administrators
  - Just enough network access to fix the issue
- Once resolved, try again
  - May require additional fixes

2.1 - Mail Gateways

Mail gateways
- Unsolicited email
  - Stop it at the gateway before it reaches the user
  - On-site or cloud-based

Email filtering
- Inbound and outbound email
  - Examine the traffic
- Unsolicited email advertisements - Spam
- Control of phishing attempts
  - Email is a large attack vector
- Anti-virus - Block bad attachments
- DLP - Data Loss Prevention
  - Block confidential information in emails



Identifying spam
- Whitelist
  - Only receive email from trusted senders
- SMTP standards checking
  - Block anything that doesn't follow RFC standards
- rDNS - Reverse DNS
  - Block email where the sender's domain doesn't match the IP address
- Tarpitting
  - Intentionally slow down the server conversation
- Recipient filtering
  - Block all email not addressed to a valid recipient email address

Email Encryption
- Mail can be easily intercepted
  - And most mail is not encrypted
- Send and receive sensitive information
  - The encryption mechanisms aren't always seamless
- Encryption can be required on the gateway
  - Based on policy
  - Force the encryption, send a password to the sender
  - Send a text message to the recipient
- Many email clients support encryption
  - Email gateway recognizes the encryption

2.1 - Other Security Devices

SSL accelerators
- You have a server farm full of web servers
- Asymmetric encryption is hard
  - Much more computationally intense than symmetric encryption
- The SSL handshake uses asymmetric encryption
  - Transfers the symmetric key using the asymmetric encryption
- Offload the handshake process to hardware
  - May use a different device
  - SSL offload, SSL termination
- Symmetric conversation continues
  - May not encrypt at all between the accelerator and the web server

SSL/TLS decryption
- Commonly used to examine outgoing SSL
  - For example, from your computer to your bank
- Wait a second. Examine encrypted traffic? Is that possible?
- SSL/TLS relies on trust
  - Without trust, none of this works

Trust me, I'm SSL
- Your browser contains a list of trusted CAs
  - My browser contains about 170 trusted CAs certificates
- Your browser doesn't trust a web site unless a CA has signed the web server's encryption certificate
  - The web site pays some money to the CA for this
  - The CA has ostensibly performed some checks
    - Validated against the DNS record, phone call, etc.
- Your browser checks the web server's certificate
  - If it's signed by a trusted CA, the encryption works seamlessly

Hardware Security Module (HSM)
- High-end cryptographic hardware
  - Plug-in card or separate hardware device

Key backup
- Secured storage

Cryptographic accelerators
- Offload that CPU overhead from other devices

Used in large environments
- Clusters, redundant power

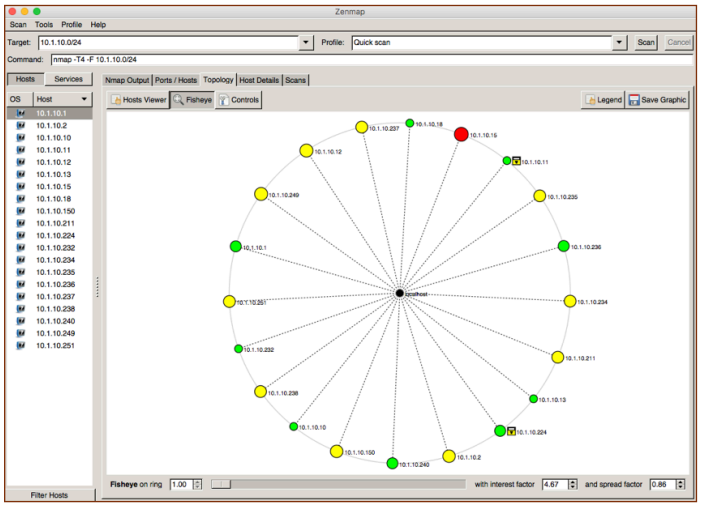
Media gateways
- Converts between PSTN (Public Switched Telephone Network) and VoIP
  - ISDN trunk on one side, Ethernet with VoIP on the other
  - SIP on one side, H.323 on the other
  - The combinations are many and varied
- Security is a significant concern
  - Disable all voice communication (DoS)
  - Make outbound calls
    - Spam, malicious services
  - Listen to voice communication
    - Corporate espionage

2.2 - Software Security Tools

Passive vs. active tools
- Passive security
  - You're a network ninja
- Watch the packets go by
  - There's a lot to learn
  - Top talkers, servers, clients, applications, operating systems, services
- Active security
  - Send traffic to a device, watch the results
  - Query a login page
  - Try a known vulnerability
  - Check account access

Protocol analyzers
- Solve complex application issues
  - Get into the details
- Gathers packets on the network
  - Or in the air
  - Sometimes built into the device
- View traffic patterns
  - Identify unknown traffic
  - Verify packet filtering and security controls
- Large scale storage
  - Big data analytics

Network scanners
- Active - scan for IP addresses and open ports
  - And operating systems, services, etc.
- Pick a range of IP addresses
  - See who responds to the scan
- Visually map the network
  - Gather information on each device
  - IP, operating system, services, etc.
- Rogue system detection
  - It's difficult to hide from a layer 2 ARP
- Nmap/Zenmap, Angry IP Scanner



Wireless scanners and crackers
- Wireless monitoring - Packet capturing
- Wireless attacks
  - Rogue access point, deauthentication attacks, etc.
- Cracking - Find a wireless network key
  - WEP - Cryptographic vulnerabilities
    - Relatively straightforward
  - WPA1 PSK and WPA2 PSK
    - Dictionary brute force, rainbow tables
- Many open source projects - Aircrack-ng Suite, Fern

Password crackers
- Passwords are stored as hashes - It's a one-way trip
- Some are stored without much complexity
  - Relatively straightforward to brute-force a weak hash
- Get the hashes - Can be the hardest part
- Use a good wordlist or use rainbow tables
  - Common passwords, multiple languages, etc.
- Many tools available
  - John the Ripper, Ophcrack

Vulnerability scanners
- Did you miss a security patch?
  - We'll find it
- Minimally invasive, but still active
  - Unlike a penetration test
- Gather as much information as possible
  - We'll separate wheat from chaff later
- Microsoft Baseline Security Analyzer, Tenable Nessus
  - Scan one or many devices
  - Automate the process, report on findings

Configuration compliance scanners
- Do your devices meet your minimum security configurations?
  - Need to comply with internal requirements or industry regulations
- Check for various configurations
  - Operating system version, installed applications, network settings, anti-virus/anti-malware settings and versions, server configurations, etc.
- Auditing may be ongoing
  - Report on current status, identify changes over time
  - Integrated with login process and/or VPN connection

Exploitation frameworks
- So many opportunities for exploits
  - The browser, operating system, applications, embedded devices, etc.
- How can you build an exploit?
  - Try many different techniques
- Many different frameworks
  - BeEF - The Browser Exploitation Framework Project
  - RouterSploit - Router Exploitation Framework
  - Metasploit - Build your own vulnerability tests or use modules in the existing exploit database

2.2 - Software Security Tools (continued)

Data sanitization tools
- Time to upgrade that hard drive
  - What happens to the data on the old drive?
- Overwrite the data once, and it's gone
  - One and done

Sanitize entire drives
  - Darik's Boot and Nuke (DBAN)
- Sanitize individual files or folders
  - Microsoft SDelete
- Don't forget about caches and temporary files
  - Data is stored in many places

Stenoganography tools
- Greek for "concealed writing"
  - Security through obscurity
- Message is invisible
  - But it's really there
- The covertext
  - The container document or file

Common steganography techniques
- Network based
  - Embed messages in TCP packets
- Use an image
  - Embed the message in the image itself
- Invisible watermarks
  - Yellow dots on printers
  - Serial number and timestamp

Honey pots
- Attract the bad guys - And trap them there
- The bad guys are probably a machine
  - Makes for interesting recon

Honeypots
- Create a virtual world to explore
- Many different options
  - http://www.projecthoneypot.org/, honeyd
- Constant battle to discern the real from the fake

Backup Utilities
- Protect from unexpected downtime
  - Malware infection, ransomware, server defacement
- Real-time file sync - rsync
- Regular partial backups
  - Hourly incremental backups
- Full backups
  - Complete file backups
  - System images
- Complete coverage, fast recovery

Banner grabbing
- Applications can be chatty
  - They sometimes say too much
- The banner is always there
  - But usually behind the scenes
- Capture it with telnet, nc, or an automated tool (i.e., Nmap)

2.2 - Command Line Security Tools

`ping`
- Test reachability
  - Determine round-trip time
  - Uses Internet Control Message Protocol (ICMP)
- One of your primary troubleshooting tools
  - Can you ping the host?
- Written by Mike Muuss in 1983
  - The sound made by sonar
  - Not an acronym for Packet INternet Groper
  - A backronym

`netstat`
- Network statistics
  - Many different operating systems
- **`netstat -a`**
  - Show all active connections
- **`netstat -b`**
  - Show binaries
- **`netstat -n`**
  - Do not resolve names

`traceroute`
- Determine the route a packet takes to a destination
  - Map the entire path
- **`tracert`** (Windows) or **`traceroute`** (POSIX)
- Takes advantage of ICMP Time to Live Exceeded error message
  - The time in TTL refers to hops, not seconds or minutes
  - TTL=1 is the first router, TTL=2 is the second router, etc.
- Not all devices will reply with ICMP Time Exceeded messages
  - Some firewalls filter ICMP
  - ICMP is low-priority for many devices

`nslookup` and `dig`
- Lookup information from DNS servers
  - Canonical names, IP addresses, cache timers, etc.
- **`nslookup`**

-Both Windows and POSIX-based
  - Lookup names and IP addresses
  - Deprecated (use dig instead)
- **`dig`** or **`DiG`** (Domain Information Groper)
  - More advanced domain information
  - Probably your first choice
  - Windows: http://www.isc.org/downloads/bind/

2.2 - Command Line Security Tools (continued)

Address Resolution Protocol
- Determine a MAC address based on an IP address
  - You need the hardware address to communicate
- **`arp -a`**
  - View local ARP table

`ipconfig` and `ifconfig`
- Most of your troubleshooting starts with your IP address
  - Ping your local router/gateway
- Determine TCP/IP and network adapter information
  - And some additional IP details
- **`ipconfig`** – Windows TCP/IP configuration
- **`ifconfig`** – Linux interface configuration

`tcpdump`
- Capture packets from the command line
  - Very convenient
- Available in most Unix/Linux operating systems
  - Included with Mac OS X, available for Windows (WinDump)
- Apply filters, view in real-time
  - Quickly identify traffic patterns
- Save the data, use in another application
  - Written in standard pcap format
- Can be an overwhelming amount of data
  - Takes a bit of practice to parse and filter

Nmap
- Network mapper
  - Find and learn more about network devices
- Port scan
  - Find devices and identify open ports
- Operating system scan
  - Discover the OS without logging in to a device
- Service scan
  - What service is available on a device? Name, version, details
- Additional scripts
  - Nmap Scripting Engine (NSE)
    - Extend capabilities, vulnerability scans

`netcat`
- "Read" or "write" to the network
  - Open a port and send or receive some traffic
- Many different functions
  - Listen on a port number
  - Transfer data
  - Scan ports and send data to a port
- Become a backdoor
  - Run a shell from a remote device
- Other alternatives and OSes - Ncat

2.3 - Common Security Issues

Unencrypted credentials
- Authentication is a critical process
  - All data must be protected
- Some protocols aren't encrypted
  - All traffic sent in the clear
  - Telnet, FTP, SMTP, IMAP
- Verify with a packet capture
  - View everything sent over the network

Logs and event anomalies
- Gather as much information as possible
  - Will be important later
- Many different sources
  - Switches, routers, firewalls, servers, IPS
- Use a security information and event management (SIEM) system
  - Consolidate logs and correlate data
  - Extensive reporting

Permission issues
- A simple oversight
  - A huge vulnerability
  - The door was left open - no lockpicking required
- June 2017 - 14 million Verizon records exposed
  - Third-party left an Amazon S3 data repository open
  - Researcher found the data before the bad guys
- Confirm permissions on initial configuration
  - Provide a process for changes and updates
  - Perform periodic audits

Access violations
- Segmentation fault
- Your operating system is looking out for you
  - Prevents access to a restricted area of memory
- Might be a programming error
  - A pointer to the wrong location
- Could be a security issue
  - Malware attempting to access restricted memory
  - Denial of service

Certificate issues
- A certificate should be signed by someone you trust
  - It's really someone your computer trusts
- Certificates should also be relatively new
  - You don't want certificates to get too old
- Application must perform the proper certificate checks
- February 2017 - Researcher finds seventy-six iOS apps that are missing TLS certificate checks
  - 18 million downloads - Easy to MitM attack

Data exfiltration
- Data is your most valuable asset
  - It might also be valuable to other people
- You've built a high-speed network
  - Also easy to remove through DVD-ROMs or USB flash drives
- July 2017 - Time Warner / Home Box Office
  - 1.5 terabytes of data exfiltrated
  - "HBO recently experienced a cyber incident, which resulted in the compromise of proprietary information."

Misconfigured devices
- Another example of leaving the door open
  - The bad guys walk right in
- Default username and password - Easy to authenticate
- Outdated software - Known vulnerabilities
- Running maintenance code
  - Debug information displayed to users
- Firewalls
  - Rules provide too much access
  - Can be difficult to audit with a large rule base
- Content filters
  - URLs are not specific enough
  - Some protocols not filtered (i.e., https)
- Access points
  - No encryption mechanisms
  - Open configurations from the wireless side

Weak security configurations
- Digital security works great
  - Until it doesn't work great any longer
- Too old - DES (Data Encryption Standard) encryption
  - Created in 1975, 56 bit keys
  - Small key size is easily brute-forced with today's technologies
- Encryption vulnerabilities - WEP (Wired Equivalent Privacy)
  - Initial 802.11 encryption algorithm
  - Vulnerabilities found with RC4 ciphers and IVs
- Hash collisions - SHA-1 (Secure Hash Algorithm 1)
  - Many collision attacks identified - Different documents with the same hash - No longer viable

Personnel issues
- The weakest link - People make mistakes
- Policy violations
  - It's in your Acceptable Use Policy (AUP) document
- Insider threats
  - Authenticated users have more free reign than non-authenticated
  - Important to assign the correct rights and permissions
- Social engineering
  - We're always so willing to help someone in need
  - They'll steal everything over the phone
- Social media
  - Posting of internal information
  - Public companies must not disclose meaningful information
  - Most organizations have a policy and marketing team
- Personal emails
  - Emails sent from work imply endorsement by the organization
  - Uses company resources

Unauthorized software
- You don't know where that's been
  - Malware, spyware, ransomware
- Conflicts
  - May conflict with the organization's software
- Licensing
  - You're going to pay for that, right?
- Ongoing support
  - Who's going to upgrade the unauthorized software? Security patches?
  - What happens when it stops working?

Baseline deviation
- Everything should be well documented
  - Hardware, software, network traffic patterns, data storage
- Any changes to the norm should be identified
  - And alerts should be sent immediately
- Common with VPNs
  - Security posture analysis before connecting to the network
  - If something deviates from the baseline, you must fix it
    - Anti-virus and signature version, OS patches
  - No remote access until it matches the baseline

License compliance violation
- So many software licenses
  - Operating systems, applications, hardware appliances
  - And they all license with different methodologies
- Availability
  - Everything works great when the license is valid
  - Meeting the expiration date may cause problems
  - Application may stop working completely
- Integrity
  - Data and applications must be accurate and complete
  - A missing/bad license may cause problems with data integrity

Asset management
- Identify and track computing assets
  - Usually an automated process
- Respond faster to security problem
  - You know who, what, and where
- Keep an eye on the most valuable assets
  - Both hardware and data
- Track licenses
  - You know exactly how many you'll need
- Verify that all devices are up to date
  - Security patches, anti-malware signature updates, etc.

Authentication issues
- Is someone really who they say they are?
- Number of factors
  - The more, the better
  - The more, the more chance of problems
- A lapse in any part of the authentication process can open the entire network
  - Weak passwords, not enough authentication factors, etc.

2.4 - Analyzing Security Output

Host-based IDS/IPS
- Intrusion Detection System / Intrusion Prevention System
- Started as a separate application
  - Now integrated into many "endpoint" products
- Protect based on signatures
  - Decrypted data
- Protect based on activity
  - Why are you modifying that file?

Antivirus
- The viruses are out there
  - It's just a matter of time
- From computers running Kaspersky Lab products in Q1 2017:
  - 479,528,279 malicious attacks blocked
  - 79,209,775 malicious URLs identified
  - 240,799 blocked ransomware attacks
  - 1,333,605 malicious installation packages on mobile devices
  - http://professormesser.link/q1stats
- Antivirus apps will alert and log on malicious software
  - Download or execute
  - Visit known-bad URL

File integrity check
- Operating system check
  - Are the original files still in place?
- Host based firewalls
- Protect against others on the network
  - Restrict access to your personal computer
- Protect wherever you go
  - Required for laptops and mobile devices
- Restricts by application and network port numbers
  - The firewall knows what you're doing
- Log displays connection attempts
  - Allowed and denied access

Application whitelisting / allow lists
- Decisions are made in the operating system
  - Often built-in to the operating system management
- Application hash
  - Only allows applications with this unique identifier
- Certificate
  - Allow digitally signed apps from certain publishers
- Path
  - Only run applications in these folders
- Network zone
  - The apps can only run from this network zone

Removable media control
- USB drives, portable hard drives
  - The bane of the security professional
- Malware infections
  - Drives brought from home
  - USB drives all over the parking lot
- Exfiltration - Terabytes of data that fits into your pocket
- Windows Event Log
  - Security auditing
  - View USB media use, log filenames copied to removable drives

Advanced malware tools
- Specialized removal and recovery tools
  - Malware techniques vary widely
- Malware is pervasive
  - Spreads to all parts of your operating system
- The best recovery is to delete and restore from good backup
  - You don't always have this option
- Research as much as possible
  - Gather recon from the malware tools
  - Stop it and prevent it

UTM/All-in-one security appliance
- Unified Threat Management (UTM) / Web security gateway
- URL filter / Content inspection, Malware inspection, Spam filter, CSU/DSU, Router, Switch, Firewall, IDS/IPS, Bandwidth shaper, VPN endpoint

Data Loss Prevention (DLP)
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the bad guys get it
  - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions in different places

Data Execution Prevention (DEP)
- No-eXecute bit
  - Intel calls it the XD bit (eXecute Disable)
  - AMD calls it Enhanced Virus Protection
- Designate sections of memory as executing code or data
  - Code can't run from protected memory locations
  - Prevents malware and viruses from executing
- The OS must support this feature
  - Windows calls it Data Execution Prevention (DEP)
  - Enabled automatically as a default
  - All logs are in the Event Viewer

Web application firewall (WAF)
- Not like a "normal" firewall
  - Applies rules to HTTP conversations
- Allow or deny based on expected input
  - Unexpected input is a common method of exploiting an application
- SQL injection
  - Add your own commands to an application's SQL query
- A major focus of Payment Card Industry Data Security Standard (PCI DSS)

2.5 - Mobile Device Connection Methods

Cellular networks
- Mobile devices
  - "Cell" phones
- Separate land into "cells"
  - Antenna coverages a cell with certain frequencies
- Security concerns
  - Traffic monitoring
  - Location tracking
  - Worldwide access to a mobile device

Wi-Fi
- Local network access
  - Local security problems
- Same security concerns as other Wi-Fi devices
- Data capture
  - Encrypt your data!
- Man-in-the-middle
  - Modify and/or monitor data
- Denial of service
  - Frequency interference

Satellite communications - SATCOM
- Remote locations, natural disasters
  - Standard communication won't work
- Literally talking to space
  - Satellites in a low earth orbit or geostationary
- Voice and data communication
  - Communicate from almost anywhere
- Handheld devices can be a security risk
  - Operating system vulnerabilities
  - Remote code execution
  - Similar security issues to other smartphones

Near field communication (NFC)
- Two-way wireless communication
  - Builds on RFID, which was one-way
- Payment systems
  - Google wallet and MasterCard partnership
  - Apple Pay
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

NFC security concerns
- Remote capture
  - It's a wireless network
  - 10 meters for active devices
- Frequency jamming
  - Denial of service
- Relay / Replay attack
  - Man in the middle
- Loss of RFC device control
  - Stolen/lost phone

ANT/ANT+
- Wireless sensor network protocol
  - 2.4 GHz ISM band (industrial, scientific, and medical)
  - An "Internet of Things" ultra-low-power protocol
  - Fitness devices, heart rate monitors, etc.
- A separate wireless service
  - Not 802.11 or Bluetooth
- Denial of service
  - Spectrum jamming
- Optional encryption
  - And no method to maintain integrity

IR (Infrared)
- Included on many smartphones, tablets, and smartwatches
  - Not really used much for file transfers and printing
- Control your entertainment center
  - Almost exclusively IR
- File transfers are possible
- Other phones can be used to control your IR devices

USB (Universal Serial Bus)
- Physical connectivity to your mobile device
  - USB to your computer
  - USB, Lightning, or proprietary on your phone
- Physical access is always a concern
  - May be easier to gain access than over a remote connection
- A locked device is relatively secure
  - Always auto-lock
- Mobile phones can also exfiltrate
  - Phone can appear to be a USB storage device

2.5 - Mobile Device Management

Mobile Device Management (MDM)
- Manage company-owned and user-owned mobile devices
  - BYOD - Bring Your Own Device
- Centralized management of the mobile devices
  - Specialized functionality
- Set policies on apps, data, camera, etc.
  - Control the entire remote device or a "partition"
- Manage access control
  - Force screen locks and PINs on these single user devices

Application management
- Managing mobile apps are a challenge
  - Mobile devices install apps constantly
- Not all applications are secure
  - And some are malicious
  - Android malware is a growing security concern
- Manage application use through whitelists
  - Only approved applications can be installed
  - Managed through the MDM
  - New applications must be checked and added

2.5 - Mobile Device Management (continued)

Content management
- Mobile Content Management (MCM)
  - Secure access to data
  - Protect data from outsiders
- File sharing and viewing
  - On-site content (Microsoft Sharepoint, file servers)
  - Cloud-based storage (Box, Office 365)
- Data sent from the mobile device
  - DLP (Data Loss Prevention) prevents copy/paste of sensitive data
  - Ensure data is encrypted on the mobile device
- Managed from the mobile device manager (MDM)

Remote wipe
- Remove all data from your mobile device
  - Even if you have no idea where it is
  - Often managed from the MDM
- Connect and wipe from the web
  - Nuke it from anywhere
- Need to plan for this
  - Configure your mobile device now
- Always have a backup
  - Your data can be removed at any time
  - As you are walking out the door

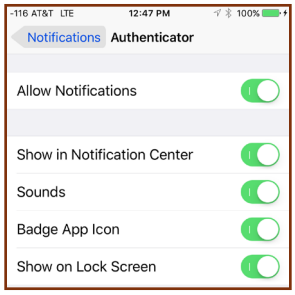
Geolocation
- Precise tracking details
  - Tracks within feet
- Can be used for good (or bad)
  - Find your phone
  - Find you
- Most phones provide an option to disable
  - Limits functionality of the phones
- May be managed by the MDM

Geofencing
- Some MDMs allow for geofencing
  - Restrict or allow features when the device is in a particular area
- Cameras
  - The camera might only work when outside the office
- Authentication
  - Only allow logins when the device is located in a particular area

Screen lock
- All mobile devices can be locked
  - Keep people out of your data
- Simple passcode or strong passcode
  - Numbers vs. Alphanumeric
- Fail too many times?
  - Erase the phone
- Define a lockout policy
  - Create aggressive lockout timers
  - Completely lock the phone

Push notification services
- Information appears on the mobile device screen
  - The notification is "pushed" to your device
- No user intervention
  - Receive notifications from one app when using a completely different app
- Control of displayed notifications can be managed from the MDM
  - Or notifications can be pushed from the MDM

Notification Options



Passwords and PINs
- The universal help desk call
  - I need to reset my password
- Mobile devices use multiple authentication methods
  - Password/passphrase, PINs, patterns
- Recovery process can be initiated from the MDM
  - Password reset option is provided on the mobile device
- MDM also has full control
  - Completely remove all security controls
  - Not the default or best practice

Biometrics
- You are the authentication factor
  - Fingerprint, face
- May not be the most secure authentication factor
  - Useful in some environments
  - Completely forbidden in others
- Availability is managed through the MDM
  - Organization determines the security of the device
- Can be managed per-app
  - Some apps require additional biometric authentication

Context-aware authentication
- Who needs 2FA?
  - The bad guys can get around anything
- Authentication can be contextual
  - If it walks like a duck…
- Combine multiple contexts
  - Where you normally login (IP address
  - Where you normally frequent (GPS information)
  - Other devices that may be paired (Bluetooth, etc.)
  - And others
- An emerging technology
  - Another way to keep data safe

2.5 - Mobile Device Management (continued)

Containerization
- Difficult to separate personal from business
  - Especially when the device is BYOD
  - Owned by the employee
- Separate enterprise mobile apps and data
  - Create a virtual "container" for company data
  - A contained area - limit data sharing
  - Storage segmentation keeps data separate
- Easy to manage offboarding
  - Only the company information is deleted
  - Personal data is retained
  - Keep your pictures, video, music, email, etc.

Full device encryption
- Scramble all of the data on the mobile device
  - Even if you lose it, the contents are safe
- Devices handle this in different ways
  - Strongest/stronger/strong ?
- Encryption isn't trivial
  - Uses a lot of CPU cycles
  - Complex integration between hardware and software
- Don't lose or forget your password!
  - There's no recovery

2.5 - Mobile Device Enforcement

Third-party app stores
- Centralized app clearinghouses
  - Apple App Store
  - Google Play
  - Microsoft Store
- Not all applications are secure
  - Vulnerabilities, data leakage
- Not all applications are appropriate for business use
  - Games, instant messaging, etc.
- MDM can allow or deny app store use

Rooting/jailbreaking
- Mobile devices are purpose-built systems
  - You don't need access to the operating system
- Gaining access
  - Android - Rooting
  - Apple iOS - Jailbreaking
- Install custom firmware
  - Replaces the existing operating system
- Uncontrolled access
  - Circumvent security features, sideload apps without using an app store
  - The MDM becomes relatively useless

Carrier unlocking
- Most phones are locked to a carrier
  - You can't use an AT&T phone on Verizon
  - Your contract with a carrier subsidizes the cost of the phone
- You can unlock the phone
  - If your carrier allows it
  - A carrier lock may be illegal in your country
- Security revolves around connectivity
  - Moving to another carrier can circumvent the MDM
  - Preventing a SIM unlock may not be possible on a personal device

Firmware OTA updates
- The operating system of a mobile device is constantly changing
  - Similar to a desktop computer
- Updates are provided over the air (OTA)
  - No cable required
- Security patches or entire operating system updates
  - Significant changes without connecting the device
- This may not be a good thing
  - The MDM can manage what OTA updates are allowed

Camera use
- Cameras are controversial
  - They're not always a good thing
  - Corporate espionage, inappropriate use
- Almost impossible to control on the device
  - No good way to ensure the camera won't be used
- Camera use can be controlled by the MDM
  - Always disabled
  - Enabled except for certain locations (geo-fencing)

SMS/MMS
- Short Message Service / Multimedia Messaging Service
  - Text messages, video, audio
- Control of data can be a concern
  - Outbound data leaks, financial disclosures
  - Inbound notifications, phishing attempts
- MDM can enable or disable SMS/MMS
  - Or only allow during certain timeframes or locations

External media
- Store data onto external or removable drives
  - SD flash memory or USB/lightning drives
- Transfer data from flash
  - Connect to a computer to retrieve
- This is very easy to do
  - Limit data written to removable drives
  - Or prevent the use of them from the MDM

2.5 - Mobile Device Enforcement (continued)

USB OTG
- USB On-The-Go
  - Connect mobile devices directly together
  - No computer required, only a cable
- The mobile device can be both a host and a device
  - Read from an external device, then act as a storage device itself
  - No need for a third-party storage device
- A USB 2.0 standard
  - Commonly seen on Android devices
- Extremely convenient
  - From a security perspective, it's too convenient

Recording microphone
- Audio recordings
  - There are microphones on every mobile device
- Useful for meetings and note taking
  - A standard for college classes
- A legal liability
  - Every state has different laws
  - Every situation is different
- Disable or geo-fence
  - Manage from the MDM

Geotagging/GPS tagging
- Your phone knows where you are
  - Location Services, GPS
- Adds your location to document metadata
  - Longitude, latitude
  - Photos, videos, etc.
- Every document may contain geotagged information
  - You can track a user quite easily
- This may cause security concerns
  - Take picture, upload to social media

WiFi Direct/ad hoc
- We're so used to access points
  - SSID configurations
- The wireless standard includes an ad hoc mode
  - Connect wireless devices directly
  - Without an access point
- WiFi Direct simplifies the process
  - Easily connect many devices together
  - Common to see in home devices
- Simplicity can aid vulnerabilities
  - Invisible access to important devices

Hotspot/tethering
- Turn your phone into a WiFi hotspot
  - Your own personal wireless router
  - Extend the cellular data network to all of your devices
- Dependent on phone type and provider
  - May require additional charges and data costs
- May provide inadvertent access to an internal network
  - Ensure proper security / passcode

Payment methods
- Send small amounts of data wirelessly over a limited area
  - Built into your phone
  - Payment systems, transportation, in-person information exchange
- A few different standards
  - Apple Pay, Android Pay, Samsung Pay
- Bypassing primary authentication would allow payment
  - Use proper security
  - Or disable completely

2.5 - Mobile Device Deployment Models

BYOD
- Bring Your Own Device / Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?

COPE
- Corporate owned, personally enabled
  - Company buys the device
  - Used as both a corporate device and a personal device
- Organization keeps full control of the device
  - Similar to company-owned laptops and desktops
- Information is protected using corporate policies
  - Information can be deleted at any time
- CYOD - Choose Your Own Device
  - Similar to COPE, but with the user's choice of device

Corporate-owned
- The company owns the device
  - And controls the content on the device
- The device is not for personal use
  - You'll need to buy your own device for home
- Very specific security requirements
  - Not able to mix business with home use

VDI/VMI
- Virtual Desktop Infrastructure / Virtual Mobile Infrastructure
  - The apps are separated from the mobile device
  - The data is separated from the mobile device
- Data is stored securely, centralized
- Physical device loss - Risk is minimized
- Centralized app development
  - Write for a single VMI platform
- Applications are managed centrally
  - No need to update all mobile devices

2.6 - Secure Protocols

Voice and video
- SRTP
  - Secure Real-Time Transport Protocol / Secure RTP
- Adds security features to RTP
  - Keep conversations private
- Encryption
  - Uses AES to encrypt the voice/video flow
- Authentication, integrity, and replay protection
  - HMAC-SHA1 - Hash-based message authentication code using SHA1

Time synchronization
- Classic NTP has no security features
  - Exploited as amplifiers in DDoS attacks
  - NTP has been around prior to 1985
- NTPsec
  - Secure network time protocol
  - Began development in June of 2015
- Cleaned up the code base
  - Fixed a number of vulnerabilities

Email
- S/MIME
  - Secure/Multipurpose Internet Mail Extensions
  - Public key encryption and digital signing of mail content
  - Requires a PKI or similar organization of keys
- Secure POP and Secure IMAP
  - Use a STARTTLS extension to encrypt POP3 with SSL or use IMAP with SSL
- SSL/TLS
  - If the mail is browser based, always encrypt with SSL

Web
- SSL/TLS
  - Secure Sockets Layer
  - Transport Layer Security
- HTTPS
  - HTTP over TLS / HTTP over SSL / HTTP Secure
- Uses public key encryption
  - Private key on the server
  - Symmetric session key is transferred using asymmetric encryption
  - Security and speed

File transfer
- FTPS
  - FTP over SSL (FTP-SSL)
  - File Transfer Protocol Secure
  - This is not SFTP
- SFTP
  - SSH File Transfer Protocol
  - Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal

LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories over an IP network
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
  - They know directories!
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, OpenLDAP, etc.

Directory services
- LDAPS (LDAP Secure)
  - A non-standard implementation of LDAP over SSL
- SASL (Simple Authentication and Security Layer)
  - Provides authentication using many different methods, i.e., Kerberos or client certificate

Remote access
- SSH (Secure Shell)
  - Encrypted terminal communication
  - Replaces Telnet

Domain name resolution
- DNS had no security in the original design
  - Relatively easy to poison a DNS
- DNSSEC
  - Domain Name System Security Extensions
- Validate DNS responses
  - Origin authentication, data integrity
- Public key cryptography
  - DNS records are signed with a trusted third party
  - Signed DNS records are published in DNS

Routing and switching
- SSH - Secure Shell - Encrypted terminal communication
- SNMPv3 - Simple Network Management Protocol version 3
  - Confidentiality - Encrypted data
  - Integrity - No tampering of data
  - Authentication - Verifies the source
- HTTPS
  - Browser-based management
  - Encrypted communication

Network address allocation
  - Securing DHCP
  - DHCP does not include any built-in security
  - There is no “secure” version of the DHCP protocol
- Rogue DHCP servers
  - In Active Directory, DHCP servers must be authorized
  - Some switches can be configured with “trusted” interfaces
  - DHCP distribution is only allowed from trusted interfaces
  - Cisco calls this DHCP Snooping

2.6 - Secure Protocols (continued)

Network address allocation
- DHCP client DoS - Starvation attack
  - Use spoofed MAC addresses to exhaust the DHCP pool
- Switches can be configured to limit the number of MAC addresses per interface
  - Disable an interface when multiple MAC addresses are seen

Subscription services
- Automated subscriptions
  - Anti-virus / Anti-malware signature updates
  - IPS updates
  - Malicious IP address databases / Firewall updates
- Constant updates
  - Each subscription uses a different update method
- Check for encryption and integrity checks
  - May require an additional public key configuration
  - Set up a trust relationship - Certificates, IP addresses

3.1 - Compliance and Frameworks

Compliance
- Compliance
  - Meeting the standards of laws, policies, and regulations
- A healthy catalog of rules
  - Across many aspects of business and life
  - Many are industry-specific or situational
- Penalties
  - Fines
  - Incarceration
  - Loss of employment
- Scope
  - Domestic and international requirements

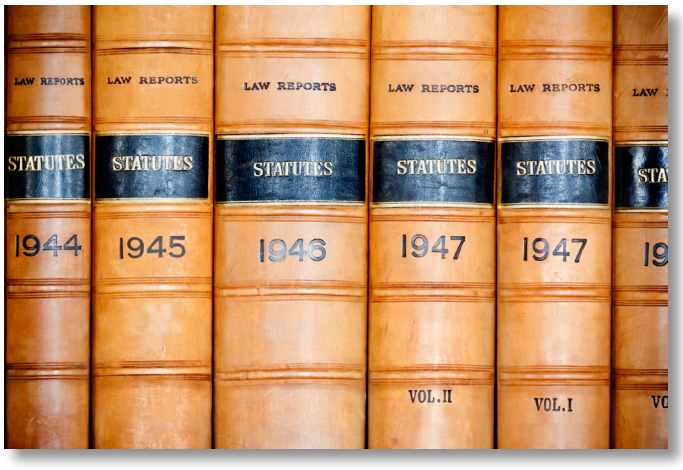
Regulatory
- Sarbanes-Oxley Act (SOX)
  - The Public Company Accounting Reform and Investor Protection Act of 2002
- The Health Insurance Portability and Accountability Act (HIPAA)
  - Extensive healthcare standards for storage, use, and transmission of health care information
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
  - Disclosure of privacy information from financial institutions

HIPPA Non-compliance penalties
- Extensive fines and penalties
- Ranges for $100 fines to $250,000
- Felony convictions include prison time

Non-regulatory
- No rule of law
  - May be strongly suggested
- A regulation may be in the works
  - Get used to the impending change
- Creates value for yourself and/or others
  - You don't need a law if it's the right thing to do
- Sharing of identified malicious IP addresses
  - There's no law or rule that requires you participate
  - It's in your best interest to share

Frameworks
- Structure and organization
  - What works best for IT?
- Process management
  - Getting the IT "product" to work best with the organization
- Best practices
  - Guidelines and examples for IT management
  - Cost effective, agile
- Lots of training
  - For everyone

Industry-specific frameworks
- COBIT
  - Control Objectives for Information and Related Technologies
  - Created by ISACA, formerly the Information Systems Audit and Control Association
  - Focus on regulatory compliance, risk management and aligning IT strategy with organizational goals
- ITIL
  - Formerly the Information Technology Infrastructure Library
  - Multiple stages of the IT lifecycle
  - Service Design, Service Transition, Service Operation, Service Strategy, Continual Service Improvement



3.1 - Secure Configuration Guides

Secure configurations
- No system is secure with the default configurations
  - You need some guidelines to keep everything safe
- Hardening guides are specific to the software or platform
  - Get feedback from the manufacturer or Internet interest group
  - They'll have the best details
- Other general-purpose guides are available online

Web server hardening
- Access a server with your browser
  - The fundamental server on the Internet
  - Microsoft Internet Information Server, Apache HTTP Server, et al.
- Huge potential for access issues
  - Data leaks, server access
- Secure configuration
  - Information leakage: Banner information, directory browsing
  - Permissions: Run from a non-privileged account, configure file permissions
  - Configure SSL: Manage and install certificates
  - Log files: Monitor access and error logs

Operating system hardening
- Many and varied
  - Windows, Linux, iOS, Android, et al.
- Updates
  - Operating system updates/service packs, security patches
- User accounts
  - Minimum password lengths and complexity
  - Account limitations
- Network access and security
  - Limit network access
- Monitor and secure
  - Anti-virus, anti-malware

Application server
- Programming languages, runtime libraries, etc.
  - Usually between the web server and the database
  - Middleware
- Very specific functionality
  - Disable all unnecessary services
- Operating system updates
  - Security patches
- File permissions and access controls
  - Limit rights to what's required
  - Limit access from other devices

Network infrastructure devices
- Switches, routers, firewalls, IPS, etc.
  - You never see them, but they're always there
- Purpose-built devices
  - Embedded OS, limited OS access
- Check with the manufacturer
  - Security updates
  - Not usually updated frequently
  - Updates are usually important

3.1 - Defense-in-Depth

Layering the defense
- Physical controls
  - Keep people away from the technology
  - Door locks, fences, rack locks, cameras
- Technical controls
  - Hardware and software to keep things secure
  - Firewalls, active directory authentication, disk encryption
- Administrative controls
  - Policies and procedures
  - Onboarding and off boarding
  - Backup media handling

Defense in depth
- Firewall
- DMZ
- Hashing passwords
- Authentication
- Intrusion prevention system
- VPN access
- Card/badge access
- Anti-virus and anti-malware software
- Security guard

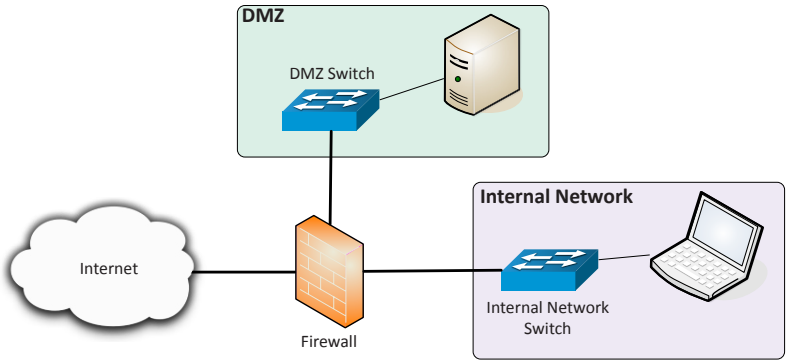
3.2 - Secure Network Topologies

Wireless networking
- The convenience of wireless
  - The security concerns of wireless
- Internal use
  - Perhaps configure a separate wireless network for guests
- Users authenticate to the wireless network
  - Use their normal network login credentials
  - 802.1X standard
  - No shared wireless passphrase
  - Integrates into the existing name services

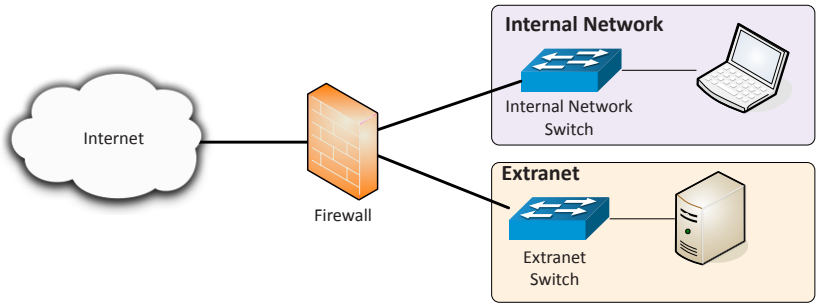
Ad hoc
- Wireless without an access point
  - Point to point communication
- Common on mobile devices
  - AirDrop, contact sharing apps
- Difficult to control on unmanaged devices
  - Configure ad hoc settings through the MDM
- Implement network access control
  - Use ad hoc, but only with the right credentials
  - Limit application use for ad hoc

3.2 - Secure Network Topologies (continued)

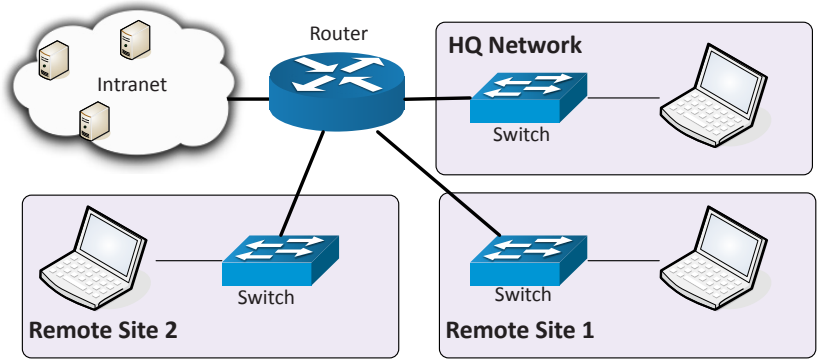
DMZ / Screened subnet
- Demilitarized zone
  - An additional layer of security between the Internet and you
  - Public access to public resources



Extranet
- A private network for partners
  - Vendors, suppliers
- Usually requires additional authentication
  - Only allow access to authorized users



Intranet
- Private network
  - Only available internally
- Company announcements, important documents, other company business
  - Employees only
- No external access
  - Internal or VPN access only



Guest network
- An optional network
  - Convenient for meetings, demonstrations, etc.
- No access to the internal network
  - Internet access only
- Integrate with a captive portal
  - Avoid unauthorized use of the network
  - Useful in congested areas
  - Keeps employees off the guest network

Honeypots and honeynets
- Attract the bad guys
  - And trap them there
- The bad guys are probably a machine
  - Makes for interesting recon
- Honeypots
  - Single-use/single-system traps
- Honeynets
  - More than one honeypot on a network
  - More than one source of information
  - http://www.projecthoneypot.org/

NAT - Network Address Translation
- It is estimated that there are over 20 billion devices connected to the Internet (and growing)
  - IPv4 supports around 4.29 billion addresses
- The address space for IPv4 is exhausted
  - There are no available addresses to assign
- How does it all work? - Network Address Translation
- This isn't the only use of NAT
  - NAT is handy in many situations

NAT and security
- NAT is not a security mechanism!
  - There's no protection there
- Security through obscurity
  - The premise: If you can't see it, you can't attack it
  - This isn't security at all
- Bad guys can circumvent an unprotected NAT
  - Sophisticated attacks already assume NAT is in place
  - They will gain access to internal devices, even with NAT
- A stateful firewall is the security mechanism
  - Used in conjunction with NAT to provide security

3.2 - Network Segmentation

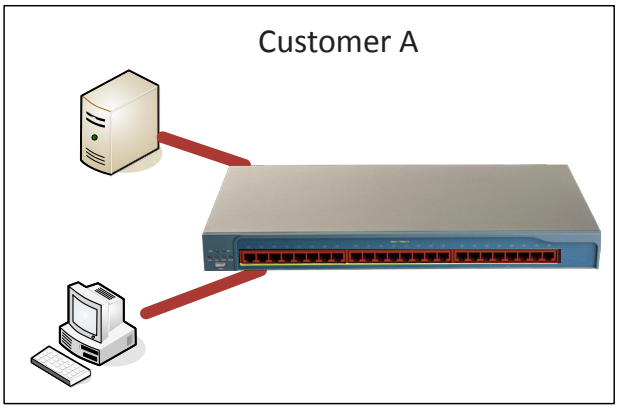
Segmenting the network
- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applications in the core are SQL and SSH
- Compliance
  - Mandated segmentation (PCI compliance)
  - Makes change control much easier

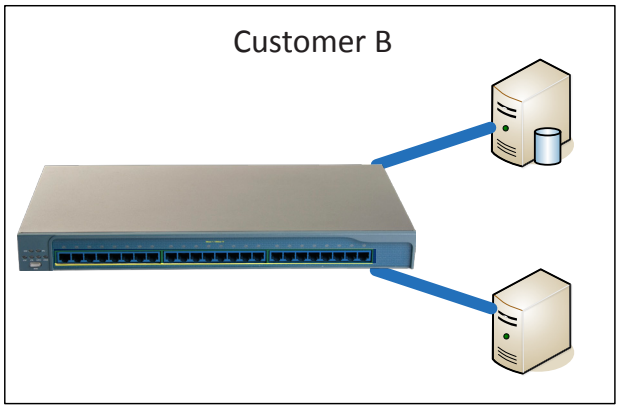
Physical segmentation
- Devices are physically separate
  - Switch A and Switch B
- Must be connected to provide communication
  - Direct connect, or another switch or router
- Web servers in one rack
  - Database servers on another
- Customer A on one switch, customer B on another
  - No opportunity for mixing data
- Separate devices
  - Multiple units, separate infrastructure

Virtualization
- Get rid of physical devices
  - All devices become virtualized
- Servers, switches, routers, firewalls, load balancers
  - All virtual devices
- Instant and complete control
  - Build a new network
  - Route between IP subnets
  - Drop a firewall between
  - Drag and drop devices between networks

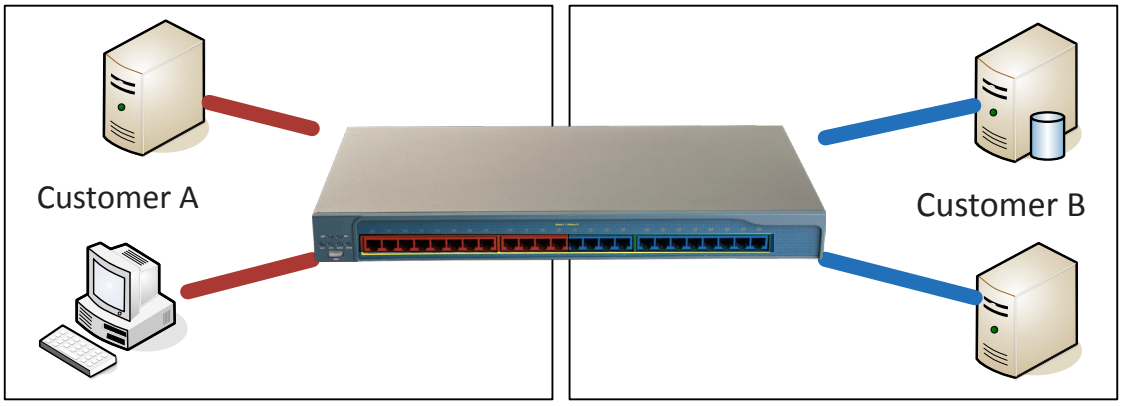
Air gaps
- One step farther than physical segmentation
  - Physical segmentation usually has some connectivity
- Remove any connectivity between components
  - No possible way for one device to communicate to another
  - No shared components
- Network separation
  - Secure networks
  - Industrial systems (SCADA, manufacturing)
- Some technologies can jump the gap
  - Removable media

Physical segmentation
- Separate Device
  - Multiple units, separate infrastructure



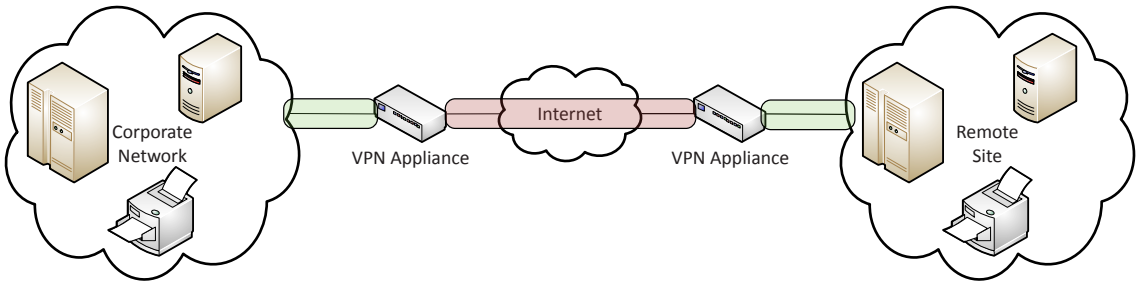


Logical segmentation with VLANs
- Virtual Local Area Networks (VLANs)
  - Separated logically instead of physically - Cannot communicate between VLANs without a Layer 3 device / router

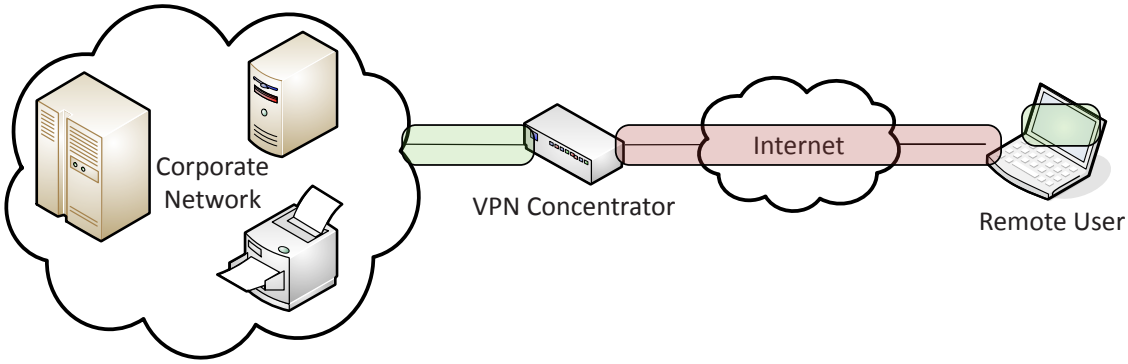


3.2 - VPN Technologies

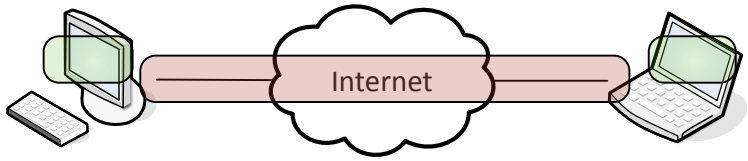
Site-to-Site VPNs
- Encrypt traffic between sites
  - Through the public Internet
- Use existing Internet connection
  - No additional circuits or costs



Host-to-Site VPNs
- Also called "remote access VPN"
- Requires software on the user device
  - May be built-in to existing operating system



Host-to-Host VPNs
- User to user encryption
- Software-based
  - No hardware needed



3.2 - Security Technology Placement

Sensors and collectors
- Gather information from network devices
  - Built-in sensors, separate devices
  - Integrated into switches, routers, servers, firewalls, etc.
- Sensors
  - Intrusion prevention systems, firewall logs, authentication logs, web server access logs, database transaction logs, email logs
- Collectors
  - Proprietary consoles (IPS, firewall), SIEM consoles, syslog servers
  - Many SIEMs include a correlation engine to compare diverse sensor data

Filters and firewalls
- Packet filters
  - Simple data blocks - ignores state
  - Linux iptables - filter packets in the kernel
  - Usually placed on a device or server
- Firewalls
  - State-based
  - Advanced filtering by IP address, port, application, content
  - Usually located on the ingress/egress of a network
  - Some organizations place them between internal networks

Proxy servers
- An intermediate server
  - Client makes the request to the proxy
  - The proxy performs the actual request
  - The proxy provides results back to the client
- Useful features
  - Access control, caching,
- URL filtering, content scanning

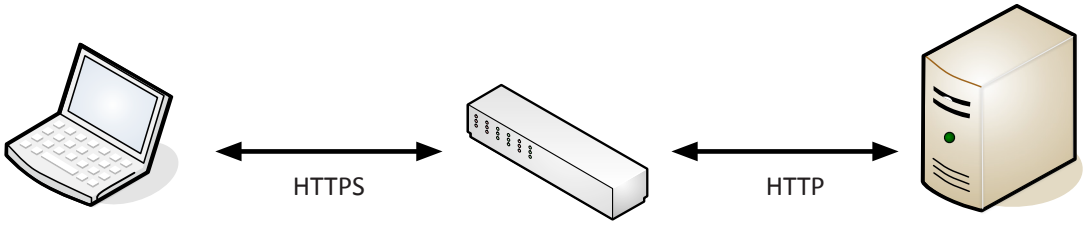
Forward proxy
- Protect users from the Internet

VPN concentrators
- VPN appliances are usually located on the edge of the network
  - Internet-facing
- Sites connect from one site to another across the Internet

Load balancers
- Manage the load across multiple devices
  - The user has no idea
  - Placed between the users and the service
- Servers can be added and removed
  - Real-time response to load
- Load balancer performs constant health checks
  - If a server disappears, it is removed from the rotation

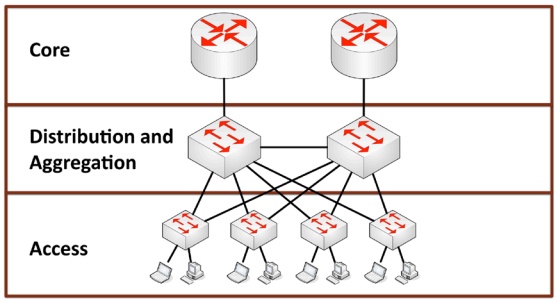
3.2 - Security Technology Placement (continued)

SSL accelerators
- The SSL handshake requires some cryptographic overhead
  - A lot of CPU cycles
- Offload the SSL process to a hardware accelerator
  - Often integrated into a load balancer

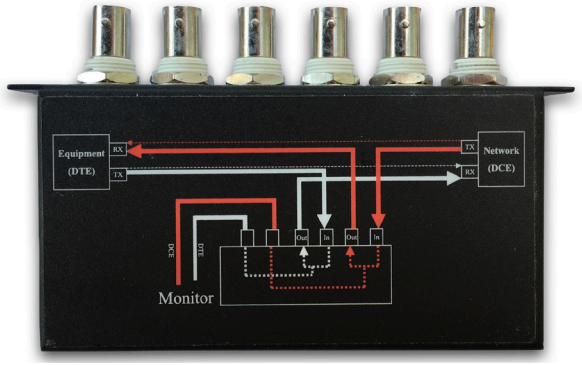


DDoS mitigation
- Resist a distributed denial of service attack
  - Minimize the impact
- Cloud-based
  - Internet provider or reverse proxy service
- On-site tools
  - DDoS filtering in a firewall or IPS
- Positioned between you and the Internet
  - Literally you against the world

Aggregation switches



Taps and port mirrors
- Intercept network traffic
  - Send a copy to a packet capture device
- Physical taps
  - Disconnect the link, put a tap in the middle
  - Can be an active or passive tap
- Port mirror
  - Port redirection, SPAN (Switched Port ANalyzer)
  - Software-based tap
  - Limited functionality, but can work well in a pinch



3.2 - Securing SDN

SDN (Software Defined Networking)
- Networking devices have two functional planes of operation
  - Control plane, data plane
- Directly programmable
  - Configuration is different than forwarding
- Agile
  - Changes can be made dynamically
- Centrally managed
  - Global view, single pane of glass
- Programmatically configured
  - Orchestration
  - No human intervention
- Open standards / vendor neutral
  - A standard interface to the network

3.3 - Hardware Security

Full Disk Encryption (FDE) / Self-Encrypting Drive (SED)
- Encrypt an entire drive
  - Not just a single file
- Protects all of your data
  - As well as the operating system
- Lose you laptop?
  - Doesn't matter without the password
- Data is always protected
  - Even if the physical drive is moved to another computer
- Built-in to the operating system
  - Microsoft BitLocker, Apple FileVault, Linux Unified Key Setup (LUKS)

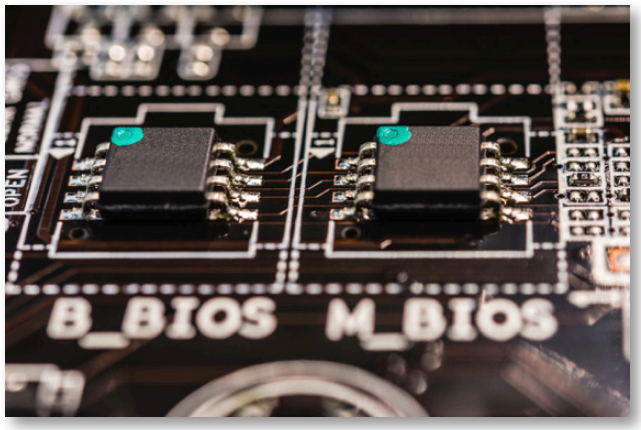
Trusted Platform Module (TPM)
- A specification for cryptographic functions
  - Hardware to help with all of this encryption stuff
- Cryptographic processor
  - Random number generator, key generators
- Persistent memory
  - Comes with unique keys burned in during production
- Versatile memory
  - Storage keys, hardware configuration information
- Password protected
  - No dictionary attacks

3.3 - Hardware Security (continued)

Hardware Security Module (HSM)
- High-end cryptographic hardware
  - Plug-in card or separate hardware device
- Key backup
  - Secured storage
- Cryptographic accelerators
  - Offload that CPU overhead from other devices
- Used in large environments
  - Clusters, redundant power

Hardware root of trust
- Security is based on trust
  - Is your data safely encrypted?
  - Is this web site legitimate?
- The trust has to start somewhere
  - TPM, HSM
  - Designed to be the hardware root of the trust
- Difficult to change or avoid
  - It's hardware
  - Won't work without the hardware

UEFI BIOS
- Unified Extensible Firmware Interface
  - Based on Intel's EFI (Extensible Firmware Interface)
- A defined standard
  - Implemented by the manufacturers
- Designed to replace the legacy BIOS
  - Need a modern BIOS for modern computers



Secure Boot
- Malicious software can "own" your system
  - Malicious drivers or OS software
- Secure boot - Part of the UEFI specification
- Digitally sign known-good software
  - Cryptographically secure
  - Software won't run without the proper signature
- Support in many different operating systems
  - Windows, Linux Fedora, openSUSE, Ubuntu
  - Apple uses their own EFI implementation

Remote attestation
- Nothing on this computer has changed
  - There have been no malware infections
  - How do you know?
- Easy when it's just your computer
  - More difficult when there are 1,000
- Remote attestation
  - Device provides an operational report to a verification server
  - Encrypted and digitally signed with the TPM
  - Changes are identified and managed

Supply chain
- September 2015: Hundreds of Cisco routers infected with "SYNful Knock"
  - Firmware modified for back-door access
- Can you trust your new server/router/switch/firewall?
  - Supply chain cyber security
- Use trusted vendors
- Critical devices should not be connected to the outside
- Verify your hardware is genuine

EMI/EMP
- Electromagnetic interference /Electromagnetic pulse
- EMI leakage
  - Determine data streams based on EMI emissions
  - Keyboards, hard drives, network connections
- Modify the security by injecting EMI
  - Change sensor data and other input
- Shielding against EMP
  - Important for national security and infrastructure

3.3 - Operating System Security

Operating system types
- There's a little overlap in most operating systems
- Network
  - Supports servers, workstations, and other network-connected devices
- Server
  - Designed to operate as a server
  - Web server, database server
- Workstation
  - Optimized for user applications
  - Email, browsing, office apps, video editing

Operating system types
- Appliance
  - Purpose-built
  - Usually a minimal OS, often unseen by the user
- Kiosk
  - Public device
  - OS is tightly locked down
- Mobile OS
  - Designed for touch screen phones and tablets
  - Optimized for mobile hardware

Patch management
- Incredibly important
  - System stability, security fixes
- Service packs
  - All at once
- Monthly updates - Incremental (and important)
- Emergency out-of-band updates
  - Zero-day and important security discoveries

Update options
- Windows update
  - Bring Windows up-to-date on each workstation
- Windows Server Update Services (WSUS)
  - Centralized management for Windows devices
- Mac OS
  - Software Update
  - Available on the Apple menu
- Linux - Many different options
  - yum, atp-get, rpm, graphical front-ends

The patching process
- Not always seamless
  - May take some planning
- May introduce other problems
  - The fix can cause another problem
- Pick and choose
  - You don't have to install every single patch
- Often centrally managed
  - The update server determine when you patch
  - Test all of your apps, then deploy
  - Efficiently manage bandwidth

Disabling unnecessary services
- "Unnecessary" isn't always obvious
  - Windows XP included almost 90 services by default, Windows 7 has over 130
- Every service has the potential for trouble
  - The worst vulnerabilities are 0-day
- This may require a lot of research
  - Many different sources
  - Don't rely on the manufacturer
- Trial and error may be necessary
  - Testing and monitoring

Least functionality
- Limit the operating system to only what's needed
  - Every function has a potential security risk
- May be different depending on the use
  - Shipping / receiving vs. IT development vs. a kiosk
- Extensive configurations
  - Disable printer installation
  - Disable changing system time
  - Disable taking ownership of file system objects
  - Deny log on as a service

Secure configurations
- Fine tuning of the operating system
  - Make your least functionality very secure
- These will apply regardless of the system use
  - The operating system is common to all
- Example secure configuration policies
  - Stay updated with the latest patches
  - Compromised systems are re-imaged (not "cleaned")
  - Changes to the standard build must go through change management
  - Perform regular integrity checks of operating system files

Evaluation Assurance Level
- Common Criteria for Information Technology Security Evaluation
  - Also called Common Criteria (or CC)
  - An international computer security certification standard (ISO/IEC 15408)
  - A common reference for US Federal Government
- Evaluation Assurance Level (EAL)
  - EAL1 through EAL7
- Trusted operating system
  - The operating system is EAL compliant
  - EAL4 is the most accepted minimum level

Application whitelisting (allow list)/ blacklisting (deny list)
- Any application can be dangerous
  - Vulnerabilities, trojan horses, malware
- Security policy can control app execution
  - Whitelisting and blacklisting
- Whitelisting / allow list
  - Nothing runs unless it's approved - Very restrictive
- Blacklisting / deny list
  - Nothing on the "bad list" can be executed
  - Anti-virus, anti-malware

Examples of application management
- Decisions are made in the operating system
  - Often built-in to the operating system management
- Application hash
  - Only allows applications with this unique identifier
- Certificate
  - Allow digitally signed apps from certain publishers
- Path - Only run applications in these folders
- Network zone
  - The apps can only run from this network zone

Disabling unnecessary accounts
- All operating systems include other accounts
  - guest, root, mail, etc.
- Not all accounts are necessary
  - Disable/remove the unnecessary
- Disable interactive logins
  - Not all accounts need to login

3.3 - Peripheral Security

Wireless keyboards and mice
- Many wireless keyboards and mice communicate in the clear
  - Use proprietary wireless communication protocols
  - Over 2.4 GHz frequencies
- Easy to capture keystrokes with a receiver
  - Inject keystrokes and mouse movements
  - Control the computer remotely
  - Vulnerability called “KeySniffer”
- Some keyboard manufacturers support AES encryption

Displays
- Electromagnetic radiation
  - View information on a screen by eavesdropping the EM signals
  - Internal signals of a laptop or external cable
  - Eavesdrop through the walls
- Firmware hacks
  - Many displays have no security for firmware upgrades
  - Log information on the screen
  - Ransomware with an LCD display

WiFi- enabled microSD
- Combination SD flash storage device and 802.11 Wi-Fi file transfers
  - Transfer from a camera to a computer without removing the SD card
- SD card authentication vulnerabilities
  - Predictable access, easy to read files over Wi-Fi
- API access to the SD card
  - Manufacturer must implement strong security
  - API access can result in data leakage or data loss

Printers/multi-function devices
- Multi-function devices
  - Printer, scanner, fax
  - Network connectivity
  - Local storage
- Reconnaissance
  - Log files for all activity, address books
- Unauthorized access
  - Print without authentication
  - Capture spool files

External storage devices
- Storage outside the computer, and often removable
  - Very portable, easy to move large files
- No authentication
  - Anyone can connect and read
  - Always use file/volume encryption
- Often used for exfiltration of data
  - Manage the use of removal storage

Digital cameras
- Capture still images and video
  - Save to digital storage
- Device operates as external storage
  - Easy to move data around
- Camera firmware can be compromised
  - Security cameras are also vulnerable

3.4 - Secure Deployments

Development to production
- Your programming team has been working on a new application
  - How will you deploy it safely and reliably?
- Patch Tuesday
  - Test and deploy Wednesday? Thursday? Friday?
- Manage the process
  - Safely move from a non-production phase to full production

Sandboxing
- Isolated testing environment
  - No connection to the real world or production system
  - A technological safe space
- Use during the development process
  - Try some code, break some code, nobody gets hurt
- Incremental development
  - Helps build the application

Working environments
- Development
  - Secure environment
  - Writing code
  - Developers test in their sandboxes
- Test - Still in the development stage
  - All of the pieces are put together
  - Does it all work?
  - Functional tests, quality assurance (QA) testing
  - If it works in test, then it’s ready for staging
- Staging - Almost ready to roll it out
  - Works and feels exactly like the production environment
  - Working with a copy of production data
  - Run performance tests
  - Test usability and features
- Production - Application is live
  - Rolled out to the user community

Secure baselines
- The security of an application environment should be well defined
  - All application instances must follow this baseline
  - Firewall settings, patch levels, OS file versions
  - May require constant updates
- Integrity measurements check for the secure baseline
  - These should be performed often
  - Check against well-documented baselines
  - Failure requires an immediate correction

3.5 - Embedded Systems

SCADA/ICS
- Supervisory Control and Data Acquisition System
  - Large-scale, multi-site Industrial Control Systems (ICS)
- PC manages equipment
  - Power generation, refining, manufacturing equipment
- Distributed control systems
  - Real-time information
  - System control
- Requires extensive segmentation
  - No access from the outside

Smart devices/IoT (Internet of Things)
- Wearable technology
  - Glasses, watches, health monitors
  - Early generation products
  - Track our location
  - Where is that data and how is it stored?
- Home automation
  - Video doorbells
  - Internet-connected garage door openers
  - Heating and cooling
  - It knows when you are home (and when you aren't)

HVAC
- Heating, Ventilating, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- PC manages equipment
  - Makes cooling and heating decisions for workspaces and data centers
- Traditionally not built with security in mind
  - Difficult to recover from an infrastructure DoS

SoC (System on a Chip)
- Multiple components running on a single chip
  - Common with embedded systems
- Small form-factor
  - External interface support
  - Cache memory, flash memory
  - Usually lower power consumption
- Security considerations are important
  - Difficult to upgrade hardware
  - Limited off-the-shelf security options

RTOS (Real-TIme Operating System)
- An operating system with a deterministic processing schedule
  - No time to wait for other processes
  - Industrial equipment, automobiles,
  - Military environments
- Extremely sensitive to security issues
  - Non-trivial systems
  - Need to always be available
  - Difficult to know what type of security is in place

Printers, scanners, and fax machines
- All-in-one or multifunction devices (MFD)
  - Everything you need in one single device
- No longer a simple printer
  - Very sophisticated firmware
- Some images are stored locally on the device
  - Can be retrieved externally
- Logs are stored on the device
  - Contain communication and fax details

Camera systems
- Video monitoring for home or office
  - 24 hour / 7 day video (and audio)
- Video recorders are IP devices
  - Authenticate using a specialized application
- Cameras are IP devices
  - 4K/high definition
- Privacy concerns
  - Don't need to ring a doorbell
  - We know when you are home
  - We might even see you

Special purpose
- Medical devices
  - Heart monitors, insulin pumps
  - Often use older operating systems
- Vehicles
  - Internal network is often accessible from mobile networks
  - Control internal electronics
  - Disable the engine
- Aircraft/UAV (Unmanned aerial vehicle)
  - DoS could damage the aircraft and others on the ground

3.6 - Development Life-Cycle Models

Building an application
- Systems development life cycle
  - Or application development life cycle
- Many ways to get from idea to app
  - And many moving parts
  - Customer requirements
  - Keep the process on schedule
  - Stay in budget
- There's no "best way"
  - But it helps to have a framework
  - There are many options

Waterfall
- Sequential design process
  - First step, then second step, then third step…
  - Considered to be the traditional model
  - Many different flavors of waterfalls

3.6 - Development Life-Cycle Models (continued)

- The waterfall
  - Requirements: Document the request
  - Analysis: Build models and business rules
  - Design: Pick a software architecture
  - Coding: Development and integration work
  - Testing: Debug the application
  - Operations: Install and support the application

Agile

- Ready, shoot, aim. Repeat.
  - It's better to get moving than to wait around
- Everyone works together
  - Co-location and pair programming
- Get some code out there
  - An app under construction is better than slideware
- Customer collaboration - Constant communication
- Quick response to change - Development is continuous

3.6 - Secure DevOps

DevOps

- Development and Operations
  - Bring together the two sides of the house
- Create and deploy
  - Speed, availability, and security
- Emphasis on automation and monitoring
  - Integration, testing, release, and manage
- Shrink deployment cycles
  - And increase the frequency of deployments
- How do you do this safely?

Security automation

- Automation is relatively inexpensive
  - It's automated, so run them early and often
- Functional security tests
  - Login, logout, ensure a secure platform
- Test against known vulnerabilities
  - Misconfigurations, weak SSL ciphers, etc.
- Penetration testing
  - Test the OS and application services
- Test the application
  - Manipulate the application to get unexpected results

Continuous integration

- Code is constantly written
  - And merged into the central repository many times a day
- So many chances for security problems
  - Security should be a concern from the beginning
- Basic set of security checks during development
  - Documented security baselines as the bare minimum
- Large-scale security analysis during the testing phase
  - Significant problems will have already been covered

Immutable systems

- Update an application every week for a year
  - It's nothing like the original deployment
  - You couldn't rebuild it if you had to
  - Configuration drift
- Immutable systems
  - Locked down and unable to change
- To update an application, a new iteration is deployed
  - The entire iteration is up to date and tested
- Much stronger security posture
  - Test and validate without worrying about a change

Infrastructure as code (IAC)

- Cloud computing
  - Relies on automation
- If you can automate it, you can quickly and safely deploy it
  - Except for the server hardware, switches, routers, firewalls, etc.
- Turn the infrastructure devices into code
  - Virtualize everything
  - Focus on what the application needs, rather than building the application based on available infrastructure
- A clearly defined infrastructure
  - Security is a known quantity

3.6 - Version Control and Change Management

The constant of change

- There will always be modifications, bug fixes, new features, and security patches
  - The important part is how you manage change
  - It's only chaotic if you allow it to be
- Changes during application development
  - Requires version control
- Changes to production
  - Formal change management

Version control

- Create a file, make a change, make another change, etc.
  - Track those changes, revert back to a previous version
- Commonly used in software development
  - But also in operating systems, wiki software, and cloud-based file storage
- Useful for security
  - Compare versions over time
  - Identify modifications to important files
- A security challenge
  - Historical information can be a security risk

3.6 - Version Control and Change Management (continued)

Change management

- Change control
  - A formal process for managing change
  - Avoid downtime, confusion, and mistakes
- Nothing changes without the process
  - Plan for a change
  - Estimate the risk associated with the change
  - Have a recovery plan if the change doesn't work
  - Make the change

Change management and security

- Every change has a security component
  - Each change must be evaluated separately
- Install security patches
  - Ideally makes the systems more secure
- Application update
  - New version, new code, new security concerns
- Change to the application instance
  - New servers, updated middleware, etc.
  - Everything must be evaluated together

3.6 - Provisioning and Deprovisioning

Provisioning

- Deploy an application
  - Web server, database server, middleware server, user workstation configurations, certificate updates, etc.
- Application software security
  - Operating system, application
- Network security
  - Secure VLAN, internal access, external access
- Software deployed to workstations
  - Check executables for malicious code, verify security posture of the workstation

Orchestration

- Automation is the key to cloud computing
  - Services appear and disappear automatically, or at the push of a button
- Entire application instances can be instantly provisioned
  - All servers, networks, switches, firewalls, and policies
- Instances can move around the world as needed
  - Follow the sun
- The security policies should be part of the orchestration
  - As applications are provisioned, the proper security is automatically included

Deprovisioning

- Dismantling and removing an application instance
  - All good things
- Security deprovisioning is important
  - Don't leave open holes, don't close important ones
- Firewall policies must be reverted
  - If the application is gone, so is the access
- What happens to the data?
  - Don't leave information out there

3.6 - Secure Coding Techniques

Secure coding concepts

- A balance between time and quality
  - Programming with security in mind is often secondary
- Testing, testing, testing
  - The Quality Assurance (QA) process
- Vulnerabilities will eventually be found
  - And exploited

Error and exception handling

- What happens when an error occurs?
  - "Graceful" exceptions
- Network connection fails, server hangs, database unavailable
  - Think of every possible problem
- Mishandled exceptions can allow execution of code
  - The bad guys love this
- Avoid default messages
  - You'll give away the underlying architecture

Input validation

- What is the expected input?
  - Validate actual vs. expected
- Document all input methods - Forms, fields, type
- Check and correct all input (normalization)
  - A zip code should be only X characters long with a letter in the X column
  - Fix any data with improper input
- The fuzzers will find what you missed
  - Don't give them an opening

Stored procedures

- SQL databases
  - Client sends detailed requests for data
  - 'SELECT * FROM wp_options WHERE option_id = 1'
- Client requests can be complex
  - And sometimes modified by the user
  - This would not be good
- Stored procedures limit the client interactions
  - 'CALL get_options'
  - That's it. No modifications to the query are possible.
- To be really secure, use only stored procedures
  - The application doesn't use any SQL queries

Code signing
- An application is deployed
  - Users run application executable or scripts
- So many security questions
  - Has the application been modified in any way?
  - Can you confirm that the application was written by a specific developer?
- The application code can be digitally signed by the developer
  - Asymmetric encryption
  - A trusted CA signs the developer's public key
  - Developer signs the code with their private key
  - For internal apps, use your own CA

Encryption
- If you can see the source code, you can easily look for security holes
  - Source code is closely guarded
  - Development platforms should use encryption
- If you're sending data over the network, it should be encrypted
  - Easy to grab data from the air
  - Encrypt important data
  - Some operating systems do this anyway

Obfuscation /camouflage
- Obfuscate
  - Make something normally understandable very difficult to understand
- Take perfectly readable code and turn it into nonsense
  - The developer keeps the readable code and gives you the chicken scratch
  - Both sets of code perform exactly the same way
- Helps prevent the search for security holes
  - Makes it more difficult to figure out what's happening
  - But not impossible

Code reuse/dead code
- Code reuse
  - Use old code to build new applications
  - Copy and paste
- If the old code has security vulnerabilities, reusing the code spreads it to other applications
  - You're making this much more difficult for everyone
- Dead code
  - Calculations are made, code is executed, results are tallied
  - The results aren't used anywhere else in the application
- All code is an opportunity for a security problem
  - Make sure your code is as alive as possible

Validation points
- Server-side validation
  - All checks occur on the server
  - Helps protect against malicious users
  - Bad guys may not even be using your interface
- Client-side validation
  - The end-user's app makes the validation decisions
  - Can filter legitimate input from genuine users
  - May provide additional speed to the user
- Use both
  - But especially server-side validation

Memory management
- As a developer, you must be mindful of how memory is used
  - Many opportunities to build vulnerable code
- Never trust data input
  - Malicious users can attempt to circumvent your code
- Buffer overflows are a huge security risk
  - Make sure your data matches your buffer sizes
- Some built-in functions are insecure
  - Use best practices when designing your code

Third-party libraries and SDK's
- Your programming language does everything
  - Almost
- Third-party libraries and software development kits
  - Extend the functionality of a programming language
- Security risk
  - Application code written by someone else
  - Might be secure. Might not be secure.
  - Extensive testing is required
- Balancing act
  - Application features vs. unknown code base

Data exposure
- So much sensitive data
  - Credit card numbers, social security numbers, medical information, address details, email information
- How is the application handling the data?
  - No encryption when stored
  - No encryption across the network
  - Displaying information on the screen
- All input and output processes are important
  - Check them all for data exposure

3.6 - Code Quality and Testing

Static code analyzers
- Static Application Security Testing (SAST)
  - Help to identify security flaws
- Many security vulnerabilities found easily
  - Buffer overflows, database injections, etc.
- Not everything can be identified through analysis
  - Authentication security, insecure cryptography, etc.
  - Don't rely on automation for everything
- Still have to verify each finding
  - False positives are an issue

Dynamic analysis (fuzzing)
- Send random input to an application
  - Fault-injecting, robustness testing, syntax testing, negative testing
- Looking for something out of the ordinary
  - Application crash, server error, exception
- 1988 class project at the University of Wisconsin
  - "Operating System Utility Program Reliability"
  - Professor Barton Miller
  - The Fuzz Generator

Fuzzing engines and frameworks
- Many different fuzzing options
  - Platform specific, language specific, etc.
- Very time and processor resource heavy
  - Many, many different iterations to try
  - Many fuzzing engines use high-probability tests
- Carnegie Mellon Computer Emergency Response Team (CERT)
  - CERT Basic Fuzzing Framework (BFF)
  - http://professormesser.link/bff

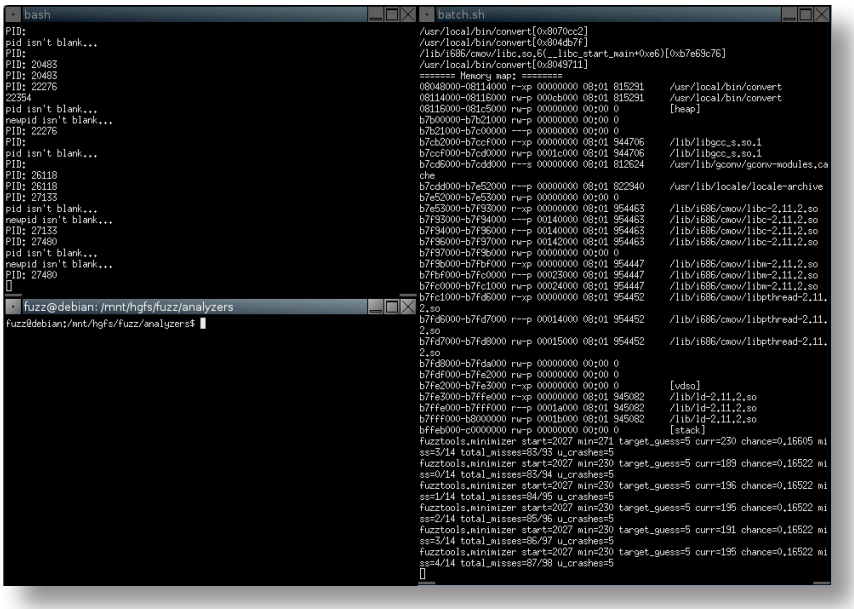
Stress testing
- The software works with one user
  - What about 1,000 users?
- Inadvertent results can occur at load
  - Unintended error messages
  - Application details and versions displayed to the user
  - Kernel and memory dumps
- Extensive automation options
  - Automate individual workstations
  - Simulate large workstation loads
  - Extensive reporting

Sandboxing
- A bit different than the developer sandbox
  - A different sandbox at a different playground
- Test environment looks and works exactly like production
  - No production systems are used
  - No production data is used
- QA can fuzz, overload, and try to break the sandboxed environment
  - You can't hurt anything in the sandbox

Model verification
- Verification and Validation (V&V)
  - You started development with a set of requirements
- Verification
  - Does the software work properly?
  - Are there any bugs to address?
  - Are we building the product right?
- Validation
  - Did you meet the high level requirements?
  - Are we building the right product?

Compiled vs. runtime code
- Compiled code
  - You don't see the source code
  - The application is an executable compiled from the source
  - The compiled code is specific to an operating system and CPU
  - Logical bugs can be identified at compile time
- Runtime code
  - Source code is usually viewable
  - The code instructions execute when the application is run
  - No opportunity to find compile-time errors, so errors are detected during or after the execution

Testing an application with a fuzzing framework



3.7 - Cloud and Virtualization Overview

Virtualization
- One computer, many operating systems
  - Mac OS X, Windows 7, Linux Ubuntu, all at the same time!
- Separate OS, independent CPU, memory, network, etc.
  - But really one computer
- Host-based virtualization
  - Your normal desktop plus others
- Standalone server that hosts virtual machines
  - Enterprise-level
- Been around since 1967 - IBM mainframe virtualization

The hypervisor
- Virtual Machine Manager
  - Manages the virtual platform and guest OSes
- May require a CPU that supports virtualization
  - Can improve performance
- Hardware management - CPU, networking, security

Hypervisors
- Type I - Bare metal, Embedded, Native
  - Run directly with hardware, no additional OS needed
- Type II - Run on a host OS
- Application containerization
  - Run an application without launching an entire VM
  - Everything you need to run the app is in the image (container/cell)

3.7 - Virtualization Security

VM sprawl avoidance
- Click a button and you've built an infrastructure
  - It becomes almost too easy to build instances
- The virtual machines are sprawled everywhere
  - You aren't sure which VMs are related to which applications
  - It becomes extremely difficult to deprovision
- Formal process and detailed documentation
  - You should have information on every virtual object

VM escape protection
- The virtual machine is self-contained
  - There's no way out - Or is there?
- Virtual machine escape
  - Break out of the VM and interact with the host operating system or hardware
- Once you escape the VM, you have great control
  - Control the host and control other guest VMs
- This would be a huge exploit
  - Full control of the virtual world

Escaping the VM
- March 2017 - Pwn2Own hacking contest
  - You pwn it, you own it - along with some cash
- JavaScript engine bug in Microsoft Edge
  - Code execution in the Edge sandbox
- Windows 10 kernel bug
  - Compromise the guest operating system
- Hardware simulation bug in VMware
  - Escape to the host
- Patches were released soon afterwards

3.7 - Cloud Deployment Models

Platform as a Service (PaaS)
- No servers, no software, no maintenance team
  - Someone else handles the platform, you handle the product
- You don't have control of the data, people, or infrastructure
- SalesForce.com is an example of PaaS

Software as a service (SaaS)
- On-demand software, no local installation
- Used for common business functions such as payroll services
- Data and applications are centrally managed
- Gmail and Google Docs is an example of SaaS

Infrastructure as a service (IaaS)
- Sometimes called Hardware as a Service (HaaS)
- Equipment is outsourced
- You are still responsible for the overall device and application management - and security
- Web hosting and email services

Cloud Deployment Models
- Private - A virtualized data center
- Public - Available to everyone over the Internet
- Hybrid - A mix of public and private
- Community - Organizations share the same resources

3.7 - Security in the Cloud

On-premises, hosted, and cloud
- On-premises - Your applications are on local hardware
  - Your servers are in your data center in your building
- Hosted - Your servers are not in your building
  - They may not even be running on your hardware
  - Usually a specialized computing environment
- Cloud - Entire application instances can be created and torn down on-demand
  - Resources are available as needed

Cloud storage
- Data is available anywhere, anytime, on any device
  - If you have a network, you have your data
- Integrates with your enterprise authentication
  - Use your network login to access your data
  - Can include two factor authentication (2FA)
- Encryption is required
  - Data is not under your direct control
  - Strong encryption mechanisms are critical

3.7 - Security in the Cloud (continued)

VDI (Virtual Desktop Infrastructure)
- Virtualize the user's desktop and run it in the data center
  - Sometimes called VDE (Virtual Desktop Environment)
- All of the computing power is in the data center
  - The end-user hardware is a "virtual desktop"
  - Relatively small computing requirements on the client workstation
  - The end-user operating system becomes less important
- Enhanced security
  - Centralized and easier to manage
  - Changes can be tightly controlled
  - The data never leaves the data center

Cloud access security broker (CASB)
- Clients are at work, data is in the cloud
  - How do you keep everything secure?
  - The organization already has well-defined security policies
- How do you make security policies work in the cloud?
  - Integrate a CASB
  - Implemented as client software, local security appliances, or cloud-based security solutions
- Visibility - Determine what apps are in use
  - Are they authorized to use the apps?
- Compliance - Are users complying with HIPAA? PCI?
- Threat prevention
  - Allow access by authorized users, stop attacks
- Data security
  - Ensure that all data transfers are encrypted
  - Protect the transfer of PII with DLP

Security as Service (SECaaS)
- Instead of managing your own security solution, move it to the cloud
  - Pay for what you use, Scale as needed
- Continuously monitoring
  - Uniformly applies to all traffic
- Anti-virus/anti-malware signatures are constantly updated
  - Block emerging threats without deploying updates

3.8 - Resiliency and Automation

Automation and scripting
- Plan for change - Implement automatically
- Automated courses of action
  - Many problems can be predicted
  - Have a set of automated responses
- Continuous monitoring
  - Check for a particular event, and then react
- Configuration validation
  - Cloud-based technologies allow for constant change
  - Automatically validate a configuration before going live
  - Perform ongoing automated checks

Templates
- Cloud orchestration relies on templates
  - Define the basic structure of an application instance
  - The blueprint of your online services
- Application instance requires a web server and a database server
  - Web server needs a specific Apache HTTP server version, a specific PHP version, SSL certs, firewall with predefined rules, brute force monitoring, etc.
- The template is just the start
  - Each application instance needs to be customized
  - Orchestrate with scripts and APIs

Master Image
- Instead of building the server each time, create a customized image
  - Build the perfect deployment
  - Save it as a master image
- You'll still need to make changes when deploying
  - IP addresses, firewall rules, licensing updates
- You'll have to keep the master image updated
  - Security patches, operating system updates, etc.
  - This can be administratively challenging

Non-persistence
- The cloud is always in motion
  - App instances are constantly built and torn down
- Snapshots capture the current configuration and data
  - Preserve the complete state of a device, or just the configuration
- Revert to known state
  - Fall back to a previous snapshot
- Rollback to known configuration
  - Don't modify the data, but use a previous configuration
- Live boot media
  - Run the operating system from removable media

Elasticity and scalability
- Elasticity - Provide resources when demand requires it
  - Scale down when things are slow
- Host availability
  - New server deployed with a few mouse clicks
- Virtualization integrates a layer of orchestration
  - Automate the deployment and movement of virtual hosts
- Servers can be added or moved to other data centers
  - All of the management systems follow the servers

3.8 - Redundancy, Fault Tolerance, and High Availability

Distributive allocation
- The bad guys are looking for your data
  - Most people keep it in the data center
- Web servers, database servers, middleware, security devices, monitoring systems
  - Many devices are required to maintain an application instance
- Don't keep everything in one place
  - Critical assets, data, and other system should be in different places
  - Makes it more difficult to target and exploit an application instance
  - A distributive allocation

Redundancy and fault tolerance
- Maintain uptime
  - The organization continues to function
- No hardware failure - Servers keep running
- No software failure - Services always available
- No system failure - Network performing optimally

Redundancy and fault tolerance
- Redundant hardware components
  - Multiple devices, load balancing power supplies
- RAID
  - Redundant Array of Independent Disks
- Uninterruptible power supplies (UPS)
  - Prepare for the disconnections
- Clustering
  - A logical collective of servers (downtime is futile)
- Load balancing
  - Shared load across components

High availability
- Redundancy doesn't always mean always available
  - May need to be enabled manually
- HA (high availability)
  - Always on, always available
- May include many different components working together
  - Watch for single points of failure

RAID Level	Description	Details
RAID 0	Striping without parity	High performance, no fault tolerance
RAID 1	Mirroring	Duplicates data for fault tolerance, but requires twice the disk space
RAID 5	Striping with parity	Fault tolerant, only requires an additional disk for redundancy
RAID 0+1, RAID 1+0, RAID 5+1, etc.	Multiple RAID types	Combine RAID methods to increase redundancy

3.9 - Physical Security Controls

Proper Lighting
- More light means more security
  - Bad guys avoid the light
  - Easier to see when lit
  - Non IR cameras can see better
- Specialized design
  - Consider overall light levels
  - Lighting angles may be important - Facial recognition
  - Avoid shadows and glare

Signs
- Clear and specific instructions
  - Keep people away from restricted areas
  - Consider visitors
- Consider personal safety
  - Fire exits
  - Warning signs (i.e., chemicals, construction)
  - Medical resources
- Informational
  - In case of emergency, call this number

Fencing
- Build a perimeter
  - Usually very obvious
  - May not be what you're looking for
- Transparent or opaque
  - See through the fence (or not)
- Robust
  - Difficult to cut the fence
- Prevent climbing
  - Razor wire
  - Build it high

Rack monitoring and security
- Monitoring systems
  - Environmental sensors
  - Webcams
  - Integration with enterprise monitoring systems
- Security
  - Closed racks
  - Locks (with keys!)
  - Fences and gates

Guards and access lists
- Security guard
  - Physical protection
  - Validates identification of existing employees
  - Provides guest access
- ID badge
  - Picture, name, other details
  - Must be worn at all times
- Access list
  - Physical list of names
  - Enforced by security guard

Alarms
- Circuit-based
  - Circuit is opened or closed
  - Door, window, fence
  - Useful on the perimeter
- Motion detection
  - Radio reflection or passive infrared
  - Useful in areas not often in use
- Duress
  - Triggered by a person
  - The big red button

Safe
- Secure your important hardware and media
  - Backups, laptops, hard drives
- Protection against the elements
  - Fire, water
- Difficult to steal
  - Very heavy
- Must be carefully managed
  - Don't share the combination
  - What happens when you lose the combination?

Locking cabinets
- Data center hardware is often managed by different groups
  - Responsibility lies with the owner
- Racks can be installed together
  - Side-to-sides
- Enclosed cabinets with locks
  - Ventilation on front, back, top, and bottom

Protected distribution
- Protected Distribution System (PDS)
  - A physically secure cabled network
- Protect your cables and fibers
  - All of the data flows through these conduits
- Prevent cable and fiber taps
  - Direct taps and inductive taps
- Prevent cable and fiber cuts
  - A physical denial of service (DoS)
- Hardened protected distribution system
  - Sealed metal conduit, periodic visual inspection

Air gap
- Physical separation between networks
  - Secure network and insecure network
  - Separate customer infrastructures
- Most environments are shared
  - Shared routers, switches, firewalls
  - Some of these are virtualized
- Specialized networks require air gaps
  - Stock market networks
  - Power systems/SCADA
  - Airplanes
  - Nuclear power plant operations

Mantraps / Access control vestibule
  - All doors normally unlocked
  - Opening one door causes others to lock
- All doors normally locked
  - Unlocking one door prevents others from being unlocked
- One door open / other locked
  - When one is open, the other cannot be unlocked
- One at a time, controlled groups
  - Managed control through an area

Faraday cage
- Blocks electromagnetic fields
  - Discovered by Michael Faraday in 1836
- A mesh of conductive material
  - The cage cancels the electromagnetic field's effect on the interior
  - The window of a microwave oven
- Not a comprehensive solution
  - Not all signal types are blocked
  - Some signal types are not blocked at all
- Can restrict access to mobile networks
  - Some very specific contingencies would need to be in place for emergency calls

Door access controls
- Conventional
  - Lock and key
- Deadbolt
  - Physical bolt
- Electronic
  - Keyless
- Token-based
  - Magnetic swipe card or proximity reader
- Multi-factor
  - Smart card and PIN

3.9 - Physical Security Controls (continued)

Biometrics
- Biometric authentication
  - Fingerprint, iris, voiceprint
- Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

Barricades/bollards
- Prevent access
  - There are limits to the prevention
- Channel people through a specific access point
  - And keep out other things
  - Allow people, prevent cars and trucks
- Identify safety concerns
  - And prevent injuries
- Can be used to an extreme
  - Concrete barriers / bollards
  - Moats

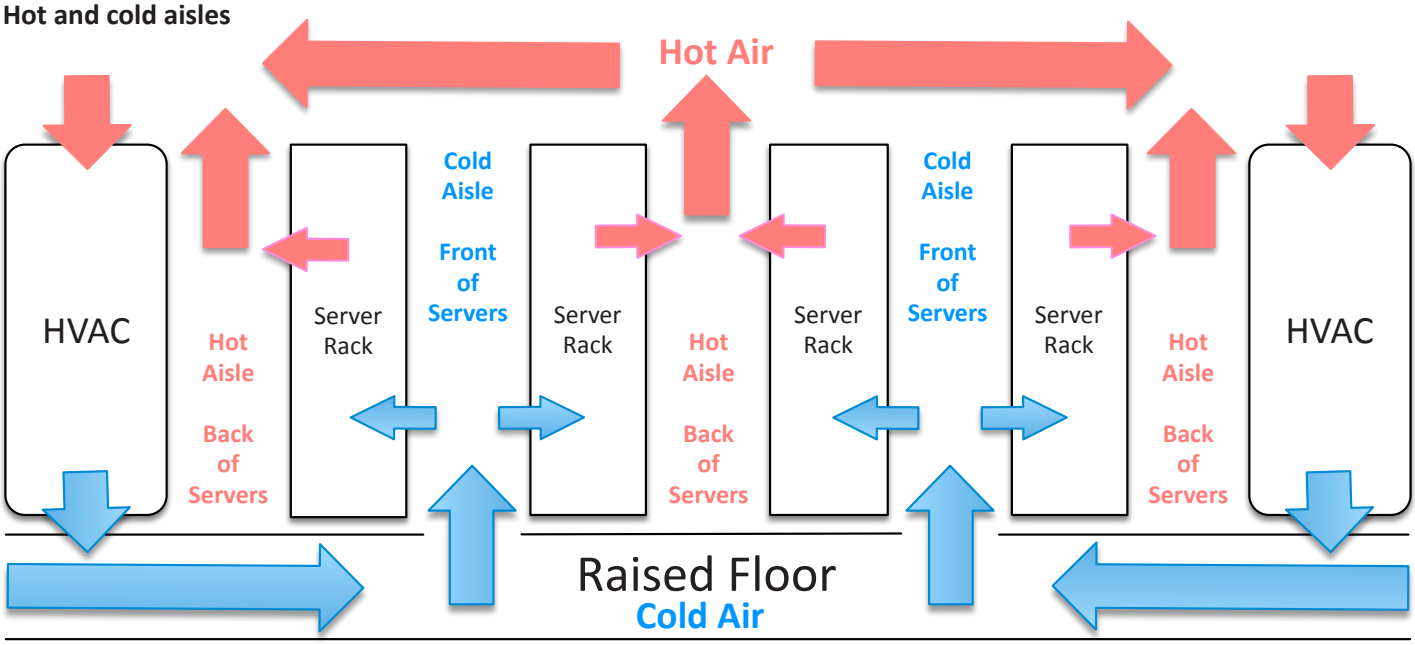
Token and cards
- Smart card
  - Integrates with devices
  - May require a PIN
- USB token
  - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone
  - SMS a code to your phone

HVAC
- Heating, Ventilating, and Air Conditioning
  - Thermodynamics, fluid mechanics, and heat transfer
- A complex science
  - Not something you can properly design yourself
  - Must be integrated into the fire system
- Data center should be separate from the rest of the building
  - Not too cold, not too hot
  - Overheating is a huge issue
- Closed-loop recirculating and positive pressurization
  - Recycle internal air, and air is pushed out

Fire suppression
- Electronics require unique responses to fire
  - Water is generally a bad thing
- Detection
  - Smoke detector, flame detector, heat detector
- Suppress with water
  - Dry pipe, wet pipe, pre-action
- Suppress with chemicals
  - Halon - No longer manufactured
  - Dupont FM-200 / American Pacific Halotron

Cable locks
- Temporary security
  - Connect your hardware to something solid
- Cable works almost anywhere
  - Useful when mobile
- Most devices have a standard connector
  - Reinforced notch
- Not designed for long-term protection
  - Those cables are pretty thin

Hot and cold aisles



3.9 - Physical Security Controls (continued)

Screen filters
- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways
- Don't sit in front of me on your flight
  - I can't help myself

Video surveillance
- CCTV (Closed circuit television)
  - Can replace physical guards
- Camera properties are important
  - Focal length - Shorter is wider angle
  - Depth of field - How much is in focus
  - Illumination requirements - See in the dark
- Often many different cameras
  - Networked together and recorded over time

Logs
- Everything is logged
  - Entering the parking area
  - Identification upon entering the building
  - Badge assignment tracks door operation
- Correlate physical location with digital access
  - Someone logged into the console while in the room
- Need a formal process to collect and archive log information
  - Some of the logs are physical, some are digital
  - May fall under privacy laws

Key management
- Cryptographic key management
  - Policies for the creation and protection of important keys
- Some keys should be physically separated from the network
  - Certificate Authority (CA) root key
  - If compromised, all keys must be replaced
  - One good reason for intermediate CAs
- The root CA certificate will only be used to sign other intermediate CAs

4.1 - AAA and Authentication

AAA framework
- Identification
  - This is who you claim to be
  - Usually your username
- Authentication
  - Prove you are who you say you are
  - Password and other authentication factors
- Authorization
  - Based on your identification and authentication, what access do you have?
- Accounting
  - Resources used: Login time, data sent and received, logout time

Multi-factor authentication
- More than one factor
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Can be expensive - Separate hardware tokens
- Can be inexpensive - Free smartphone applications

Something you are
- Biometric authentication
  - Fingerprint, iris, voiceprint
- Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

Something you have
- Smart card
  - Integrates with devices
  - May require a PIN
- USB token - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone
  - SMS a code to your phone

Something you know
- Password
  - Secret word/phrase, string of characters
  - Very common authentication factor
- PIN
  - Personal identification number
  - Not typically contained anywhere on a smart card or ATM card
- Pattern
  - Complete a series of patterns
  - Only you know the right format

Somewhere you are
- Provide a factor based on your location
  - The transaction only completes if you are in a particular geography
- IP address
  - Not perfect, but can help provide more info
  - Works with IPv4, not so much with IPv6
- Mobile device location services
  - Geolocation to a very specific area
  - Must be in a location that can receive GPS information or near an identified mobile or 802.11 network
  - Still not a perfect identifier of location

4.1 - AAA and Authentication (continued)

Something you do
- A personal way of doing things
  - You're special
- Handwriting analysis
  - Signature comparison
  - Writing technique
- Typing technique
  - Personal typing pattern
- Very similar to biometrics
  - Close to something you are

Federation
- Provide network access to others
  - Not just employees
  - Partners, suppliers, customers, etc.
- Third-parties can establish a federated network
  - Authenticate and authorize between the two organizations
  - Login with your Facebook credentials
- The third-parties must establish a trust relationship
  - And the degree of the trust

Single sign-on (SSO)
- Authenticate one time
  - Gain access to everything!
- Saves time
  - A seamless process
  - End-user doesn't see any of the complexities under the surface
- Many different methods
  - Kerberos authentication and authorization
  - 3rd-party options

Transitive trust
- Trust relationships need to be established early
  - Difficult to change once in place
- One-way trust
  - Domain B trusts Domain A, Domain A doesn't trust Domain B
- Two-way trust
  - Both domains are peers, both trust each other equally
- Non-transitive trust
  - A trust is specifically created and applies only to that domain
- Transitive trust
  - Domain A trusts Domain B, Domain B trusts Domain C, therefore Domain A trusts Domain C

4.2 - Identity and Access Services

RADIUS (Remote Authentication Dial-in User Service)
- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
  - Not just for dial-in
- Centralize authentication for users
  - Routers, switches, firewalls
  - Server authentication
  - Remote VPN access
  - 802.1X network access
- RADIUS services available on almost any server operating system

TACACS
- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- XTACACS (Extended TACACS)
  - A Cisco-created (proprietary) version of TACACS
  - Additional support for accounting and auditing
- TACACS+
  - The latest version of TACACS, not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP (tcp/389 and udp/389)
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, Novell eDirectory, etc.

X.500 Distinguished Names
- attribute=value pairs
- Most specific attribute is listed first
  - This may be similar to the way you already think

X.500 Directory Informational Tree
- Hierarchical structure
  - Builds a tree
- Container objects
  - Country, organization, organizational units
- Leaf objects
  - Users, computers, printers, files

4.2 - Identity and Access Services (continued)

Microsoft NTLM

- Windows challenge/response
  - Domain name, username, password hash
- LAN Manager (LANMAN)
  - Microsoft and 3Com network operating system
- NT LAN Manager v2 (NTLM) challenge/response
  - Hash challenge, similar to CHAP
  - Somewhat insecure
    - MD4 password hash (same as NTLMv1)
    - HMAC-MD5 hash of username and server name
    - Variable-length challenge of timestamp, random data, domain name

Microsoft NTLM vulnerabilities

- Some Windows password databases contain LM hash versions of the passwords
  - Compatibility with older systems
- NTLM vulnerable to a credentials forwarding attack
  - Use credentials of one computer to gain access to another
- Migrate to Kerberos
  - If you haven't already

Kerberos

- Network authentication protocol
  - Authenticate once, trusted by the system
  - No need to re-authenticate to everything
  - Mutual authentication - the client and the server
    - Protect against man-in-the-middle or replay attacks
- Standard since the 1980s
  - Developed by the Massachusetts Institute of Technology (MIT)
  - RFC 4120
- Microsoft starting using Kerberos in Windows 2000
  - Based on Kerberos 5.0 open standard
  - Compatible with other operating systems and devices

SSO with Kerberos

- Authenticate one time
  - Lots of backend ticketing
- No constant username and password input!
  - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly

4.2 - PAP, CHAP, and MS-CHAP

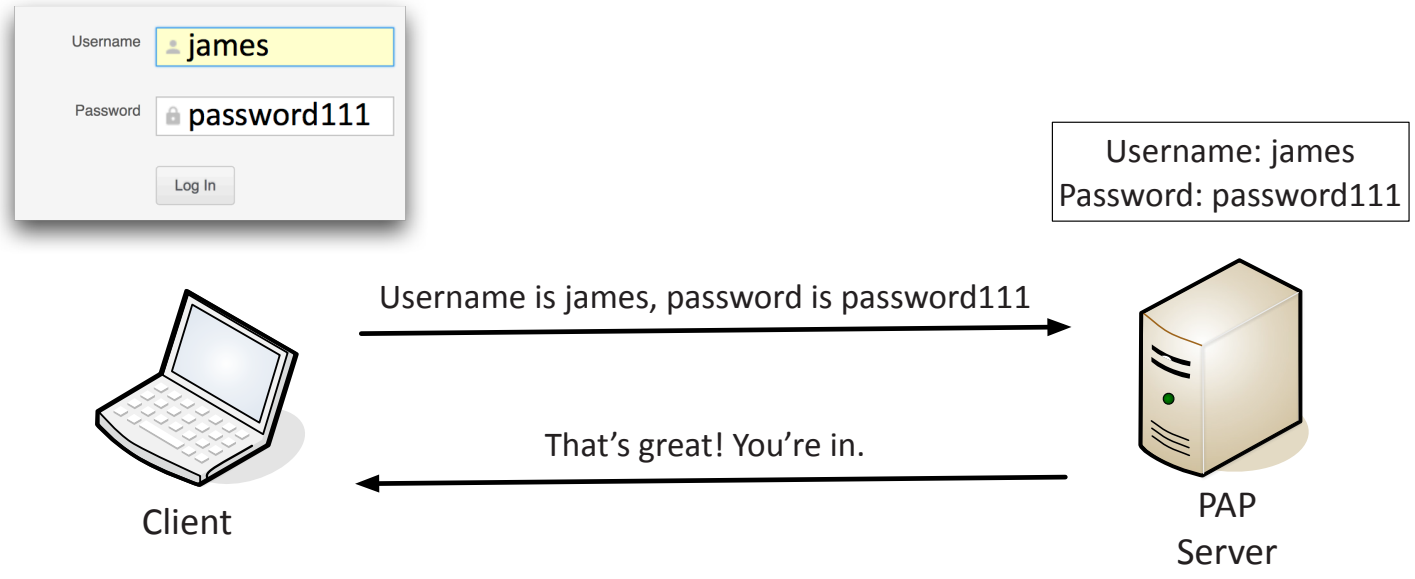
PPP authentication

- Point-to-Point Protocol
  - Analog dialup, ISDN
- And derivatives
  - PPTP (Point-to-Point Tunneling Protocol)
  - PPPoE (Point-to-Point Protocol over Ethernet)
- Need to authenticate through these non-Ethernet networks
  - PAP, CHAP, and MS-CHAP

PAP (Password Authentication Protocol)

- A basic authentication method
  - Used in legacy operating systems
  - Rare to see singularly used
- PAP is in the clear
  - Weak authentication scheme
  - Non-encrypted password exchange
  - We didn't require encryption on analog dialup lines

PAP (Password Authentication Protocol) - Authentication process



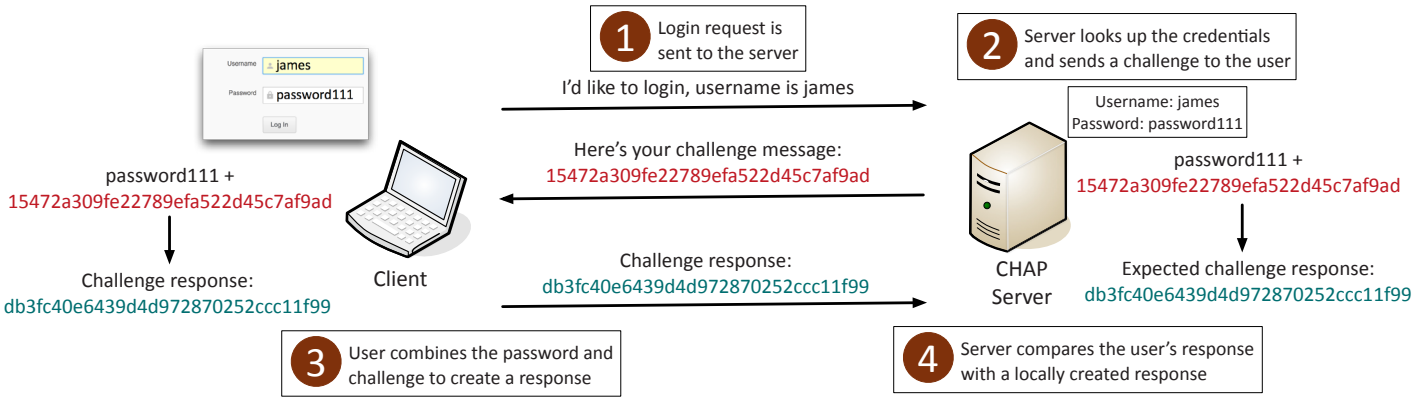
4.2 - PAP, CHAP, and MS-CHAP (continued)

CHAP

- Challenge-Handshake Authentication Protocol
  - Encrypted challenge sent over the network
- Three-way handshake
  - After link is established, server sends a challenge message
  - Client responds with a password hash calculated from the challenge and the password
  - Server compares received hash with stored hash
- Challenge-Response continues
  - Occurs periodically during the connection
  - User never knows it happens

MS-CHAP

- Microsoft's implementation of CHAP
  - Used commonly on Microsoft's Point-to-Point Tunneling Protocol (PPTP)
  - MS-CHAP v2 is the more recent version
- Security issues related to the use of DES
  - Relatively easy to brute force the 256 possible keys to decrypt the NTLM hash
  - Don't use MS-CHAP!
  - Consider L2TP, IPsec, or some other secure VPN technology



4.2 - Federated Identities

Server-based authentication

- HTTP/web browser communication is stateless
  - Each request is unique and has no relationship to the previous request
- Traditionally, the server has kept track of logins
  - You are assigned a session ID when you login
  - The server checks each time you send a request
- Adds overhead to the server
  - Difficult to scale
  - Adds challenges with redundancy and cloud services
  - Difficult to manage across multiple devices

Token-based authentication

- No session information is stored on the server
  - Stateless, just like HTTP
- After user authenticates, the application sends a token to the client
  - The client stores the token locally
- The token is provided with each request to the server
  - The server validates the token and the application continues to work normally

Federation

- Provide network access to others
  - Not just employees - Partners, suppliers, customers, etc.
  - Provides SSO and more
- Third-parties can establish a federated network
  - Authenticate and authorize between the two organizations
  - Login with your Facebook credentials
- The third-parties must establish a trust relationship
  - And the degree of the trust

Security Assertion Markup Language (SAML)

- Open standard for authentication and authorization
  - You can authenticate through a third-party
  - One standard does it all, sort of
- Shibboleth is open-source software that implements SAML to provide federated SSO
  - SAML defines the standard that Shibboleth uses
- Not originally designed for mobile apps
  - This has been SAML's largest roadblock

OAuth

- Authorization framework
  - Determines what resources a user will be able to access
- Created by Twitter, Google, and many others
  - Significant industry support
- Not an authentication protocol
  - OpenID Connect handles the single sign-on authentication
  - OAuth provides authorization between applications
- Relatively popular
  - Used by Twitter, Google, Facebook, LinkedIn, etc.

4.3 - Access Control Models

Access control
- Authorization
  - The process of ensuring only authorized rights are exercised
    - Policy enforcement
- The process of determining rights
    - Policy definition
- Users receive rights based on Access Control models
  - Different business needs or mission requirements

Mandatory Access Control (MAC)
- The operating system limits the operation on an object
  - Based on security clearance levels
- Every object gets a label
  - Confidential, secret, top secret, etc.
- Labeling of objects uses predefined rules
  - The administrator decides who gets access to what security level
  - Users cannot change these settings

Discretionary Access Control (DAC)
- Used in most operating systems
  - A familiar access control model
- You create a spreadsheet
  - As the owner, you control who has access
  - You can modify access at any time
- Very flexible access control
  - And very weak security

Role based access control (RBAC)
- You have a role in your organization
  - Manager, director, team lead, project manager
- Administrators provide access based on the role of the user
  - Rights are gained implicitly instead of explicitly
- In Windows, use Groups to provide role-based access control
  - You are in shipping and receiving, so you can use the shipping software
  - You are the manager, so you can review shipping logs

Attribute-based access control (ABAC)
- Users can have complex relationships to applications and data
  - Access may be based on many different criteria
- ABAC can consider many parameters
  - A "next generation" authorization model
  - Aware of context
- Combine and evaluate multiple parameters
  - Resource information, IP address, time of day, desired action, relationship to the data, etc.

Rule-based access control
- Generic term for following rules
  - Conditions other than who you are
- Access is determined through system-enforced rules
  - System administrators, not users
- The rule is associated with the object
  - System checks the ACLs for that object
- Rule examples
  - Lab network access is only available between 9-5
  - Only Chrome browsers may complete this web form

File system security
- Store files and access them
  - Hard drive, SSDs, flash drives, DVDs
  - Part of most operating systems
- Accessing information
  - Access control list
  - Group/user rights and permissions
  - Can be centrally administered and/or users can manage files they own
- Encryption can be built-in
  - The file system handles encryption and decryption

Database security
- Databases have their own access control
  - Username, password, permissions
- Encryption may be an option
  - Most databases support data encryption
- Data integrity is usually an option
  - No data is lost because of a fault
  - Part of the database server operation
- Applications can provide a secure front-end
  - Prevent SQL injections and inappropriate access to data

4.3 - Access Control Technologies

Proximity cards
- Close range card - Contactless smart card
- Passive device - No power in the card
  - Powered from the reader
- Not a large data storage device
  - Often used as an identifier
  - Keycard door access, library cards, payment systems
  - The identifier is linked to data stored elsewhere

Smart cards
- Integrated circuit card - -Contact or contactless
- Common on credit cards
  - Also used for access control
- Must have physical card to provide digital access
  - A digital certificate
- Multiple factors
  - Card with PIN or fingerprint

4.3 - Access Control Technologies (continued)

Biometric factors
- Fingerprint scanner
  - Phones, laptops, door access
- Retinal scanner
  - Unique capillary structure in the back of the eye
- Iris scanner
  - Texture, color
- Voice recognition
  - Talk for access
- Facial recognition
  - Shape of the face and features

Biometric acceptance rates
- False acceptance rate (FAR)
  - Likelihood that an unauthorized user will be accepted
  - This would be bad
- False rejection rate (FRR)
  - Likelihood that an authorized user will be rejected
  - No, it's really me
  - Let's try again
- Crossover error rate (CER)
  - The rate at which FAR and FRR are equal
  - Adjust sensitivity to equalize both values
  - Used to quantitatively compare biometric systems

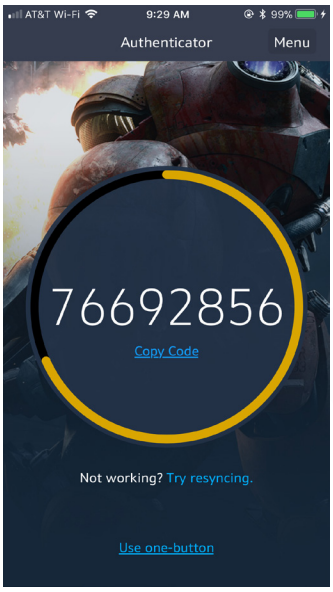
Token generators
- Pseudo-random token generators
  - A useful authentication factor
- Carry around a physical hardware token generator
  - Where are my keys again?
- Use software-based token generator on your phone
  - Powerful and convenient

HOTP
- One-time passwords
  - Use them once, and never again
  - Once a session, once each authentication attempt
- HMAC-based One-Time Password algorithm
  - Keyed-hash message authentication code (HMAC)
  - The keys are based on a secret key and a counter
- Token-based authentication
  - The hash is different every time
- Hardware and software tokens available
  - You'll need additional technology to make this work

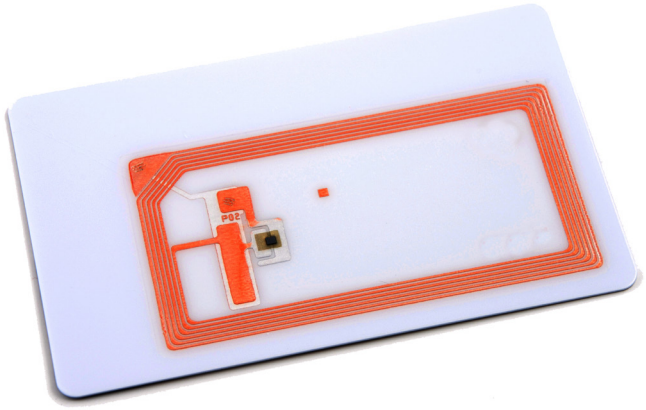
TOTP
- Time-based One-Time Password algorithm
  - Use a secret key and the time of day
  - No incremental counter
- Secret key is configured ahead of time
  - Timestamps are synchronized via NTP
- Timestamp usually increments every 30 seconds
  - Put in your username, password, and TOTP code
- One of the more common OTP methods
  - Used by Google, Facebook, Microsoft, etc.

Certificate-based authentication
- Smart card
  - Private key is on the card
- PIV (Personal Identity Verification) card
  - US Federal Government smart card
  - Picture and identification information
- CAC (Common Access Card)
  - US Department of Defense smart card
  - Picture and identification
- IEEE 802.1X
  - Gain access to the network using a certificate
  - On device storage or separate physical device

TOTP - Time-based One-time Password Algorithm
- Hardware and software token generator



Proximity cards
- Close range card
- Contactless smart card



4.4 - Account Types

User accounts
- An account on a computer associated with a specific person
  - The computer associates the user with a specific identification number
- Storage and files can be private to that user
  - Even if another person is using the same computer
- No privileged access to the operating system
  - Specifically not allowed on a user account
- This is the account type most people will use
  - Your user community

Shared and generic accounts
- Shared account
  - Used by more than one person
  - Guest login, anonymous login
- Very difficult to create an audit trail
  - No way to know exactly who was working
  - Difficult to determine the proper privileges
- Password management becomes difficult
  - Password changes require notifying everyone
  - Difficult to remember so many password changes
  - Just write it down on this yellow sticky paper
- Best practice: Don't use these accounts

Service accounts
- Used exclusively by services running on a computer
  - No interactive/user access (ideally)
  - Web server, database server, etc.
- Access can be defined for a specific service
  - Web server rights and permissions will be different than a database server
- Commonly use usernames and passwords
  - You'll need to determine the best policy for password updates

Privileged accounts
- Elevated access to one or more systems
  - Administrator, Root
- Complete access to the system
  - Often used to manage hardware, drivers, and software installation
- This account should not be used for normal administration
  - User accounts should be used
- Needs to be highly secured
  - Strong passwords, 2FA
  - Scheduled password changes

4.4 - Account Management

Least privilege
- Rights and permissions should be set to the bare minimum
  - You only get exactly what's needed to complete your objective
- All user accounts must be limited
  - Applications should run with minimal privileges
- Don't allow users to run with administrative privileges
  - Limits the scope of malicious behavior

On-boarding
- Bring a new person into the organization
  - New hires or transfers
- Technical agreements need to be signed
  - May be part of the employee handbook or a separate AUP
- Create accounts
  - Associate the user with the proper groups and departments
- Provide required IT hardware
  - Laptops, tablets, etc.
  - Preconfigured and ready to go

Off-boarding
- All good things…
  - But you knew this day would come
- This process should be pre-planned
  - You don't want to decide how to do things at this point
- What happens to the hardware and the data?
- Account information is usually deactivated
  - But not always deleted

Perform routine audits
- Is everything running to policy?
  - You have to police yourself
- It's amazing how things change
  - Make sure the routine is scheduled
- Certain actions can be automatically identified
  - Consider a tool for log analysis

Auditing
- Permission auditing
  - Does everyone have the correct permissions?
  - Some Administrators don't need to be there
  - Scheduled recertification
- Usage auditing
  - How are your resources used?
  - Are your systems and applications secure?
- Time-of-day restrictions
  - Nobody needs to access the lab at 3 AM

4.4 - Account Management (continued)

Standard naming convention
- Unique
  - The username shouldn't conflict with another user
  - Use the same username across multiple systems
- Consistent
  - Usernames shouldn't describe a role or status
- Persistent
  - Use the same username for the duration of employment
- Memorable
  - This shouldn't be difficult. Make it easy to remember

Account maintenance
- Account creation
  - Initial provisioning
  - Password management
  - Group and permission assignments
- Periodic updates
  - Password resets / forced updates
  - Permission audits
- Deprovisioning
  - Disable account
  - Archive user documents and encryption keys

Group-based access control
- Set privileges based on what you do
  - Put many users into a single group
  - Set privileges on the group
  - Add/remove users from the group to assign privileges
- Users can be members of multiple groups
  - Group permissions can overlap
  - How do you determine the effective permissions?
    - Not as straightforward as you might think

Location-based policies
- User access is based on location
  - GPS - mobile devices, very accurate
  - 802.11 wireless, less accurate
  - IP address, not very accurate
- Restrict application use
  - Don't allow this app to run unless you're near the office
- Apply security rules
  - Your IP address is associated with an IP block in China
  - We don't have an office in China
  - Permission not granted

4.4 - Account Policy Enforcement

Credential management
- All that stands between the outside world and all of the data
  - The data is everything
- Passwords must not be embedded in the application
  - Everything needs to reside on the server, not the client
- Communication across the network should be encrypted
  - Authentication traffic should be impossible to see

Configuring settings
- Windows Group Policy Management
  - Apply security and admin settings across many computers
  - Thousands of settings
- Different than NTFS or Share permissions
  - Control the use of the operating system
- Linked to Active Directory administrative boundaries
  - Sites, domains, organization units (OUs)
  - Define by groups, locations, etc.

Group Policy control
- Administrative policies
  - Remove Add or Remove Programs
  - Prohibit changing sounds
  - Allow font downloads
  - Only allow approved domains to use ActiveX controls without prompt
- Security policies
  - Specify minimum password length
  - Maximum security log size
  - Enforce user login restrictions

Password complexity and length
- Make your password strong
  - No single words
  - No obvious passwords
    - What's the name of your dog?
  - Mix upper and lower case
  - Use special characters
    - Don't replace a o with a 0, t with a 7
- A strong password is at least 8 characters
  - Consider a phrase or set of words
- Prevent password reuse
  - System remembers password history, requires unique passwords

Password expiration and recovery
- All passwords should expire
  - Change every 30 days, 60 days, 90 days
- Critical systems might change more frequently
  - Every 15 days or every week
- The recovery process should not be trivial!
  - Some organizations have a very formal process

Account lockout and disablement
- Too many bad passwords will cause a lockout
  - This should be normal for most users
  - This can cause big issues for service accounts
    - You might want this
- Disable accounts
  - Part of the normal change process
  - You don't want to delete accounts
    - At least not initially

5.1 - Agreement Types

Standard operating procedure
- Important processes to maintain data and system security
  - Detail routine operations
  - Usually quite extensive
- Day-to-day processes
- New user account creation
  - Backup data storage requirements
  - Encryption key requests
- These should be well documented
  - Some processes require extensive documentation
  - Comply with industry regulations

Interoperability agreements
- Third-parties and outsourced services
  - The legal side of information technology
- Web hosting, payroll services, firewall management, etc.
  - Some of your data is in the hands of others
  - Who do they hire?
  - What type of access controls are in place?
- Include the legal department with these agreements
  - It can only help you later

Common agreements
- Service Level Agreement (SLA)
  - Minimum terms for services provided
  - Uptime, response time agreement, etc.
- Business Partners Agreement (BPA)
  - Commonly seen between manufacturers and resellers
- Interconnection Security Agreement (ISA)
  - Used by US Federal Government to define security controls

Common agreements
- Memorandum of Understanding (MOU)
  - Both sides agree on the contents of the memorandum
  - Usually includes statements of confidentiality
  - Informal letter of intent; not a signed contract
- Memorandum of Agreement (MOA)
  - The next step above a MOU
  - Both sides agree to the objectives
  - A legal document, even without legal language
  - Unlike a contract, may not contain legally enforceable promises

5.1 - Personnel Management

Business policies
- Mandatory vacations - Rotate others through the job
  - The longer the vacation, the better chance to identify fraud
  - Especially important in high-security environments
- Job rotation
  - Keep people moving between responsibilities
  - No one person maintains control for long periods of time
- Separation of duties
  - Split knowledge
    - No one person has all of the details
    - Half of a safe combination
  - Dual control
    - Two people must be present to perform a function
    - Two keys open a safe (or launch a missile)
- Clean desk policy
  - When you leave, nothing is on your desk
  - Limit the exposure of sensitive data to third-parties

Background checks
- Background checks - Pre-employment screening
  - Verify the applicant's claims
  - Discover criminal history, workers compensation claims, etc.
  - Legalities vary by country
- Adverse actions
  - An action that denies employment based on the background check
  - May require extensive documentation
  - Can also include existing employees

Personnel security procedures
- NDA (Non-disclosure agreement)
  - Confidentiality agreement / Legal contract
  - Prevents the use and dissemination of confidential information
- Onboarding
  - Bring someone into the organization
  - Induction / Training - Usually a formal process
- Continuing education
  - Initial training isn't enough
  - Security is constantly changing

Acceptable use policies (AUP)
- What is acceptable use of company assets?
  - Detailed documentation
  - May be documented in the Rules of Behavior
- Covers many topics
  - Internet use, phones, computers, mobile devices, etc.
- Used by an organization to limit legal liability
  - If someone is dismissed, these are the well-documented reasons why

Exit interviews
- Employee is leaving - Ask them a few questions first
- Information gathered can be used for improvements or changes
  - What are your reasons for leaving?
  - What did you like most? Least?
  - What could we have improved that would have caused you to stay?
- Very formal process and statistical record keeping
  - Useful for HR to compile and track

5.1 - Role-based Awareness Training

Role-based awareness training
- Before providing access, train your users
  - Detailed security requirements
- Specialized training
  - Each user role has unique security responsibilities
- Also applies to third-parties
  - Contractors, partners, suppliers
- Detailed documentation and records
  - Problems later can be severe for everyone

Roles
- Data owner
  - Executive level manager, responsible for data security Ultimately responsible for compliance
- System administrator
  - Administrator of the systems that enable the applications and data
  - May not necessarily be a user of the app or view the data
- System owner
  - Makes decisions about the overall operation of the app and data
  - Defines security policies and backup policies
  - Manages changes and updates

User roles
- User
  - Application user
  - Has least privileged access to the application and data
- Privileged user
  - Additional application and data permissions
  - Area manager, report creation, user and password changes
- Executive user
  - Responsible for the overall operation of the application
  - High-level decision making for direction
  - Evaluates goals and makes decisions about future directions

5.1 - General Security Policies

Social media policies
- Balance the company reputation with employee participation
  - Social media use can be a great thing
- Extension of your code of conduct
  - Define requirements and expectations
  - Identification as an employee
  - Personal responsibility
- Confidential information
  - Public companies are legally bound
  - There's a company spokesperson for public comments

Personal email policies
- Qualify the use of email
  - Business use, no personal use
- Prohibit disruptive or offensive use
  - Avoid problems in the workplace
- Compliance issues
  - Some organizations are legally required to prohibit personal email
- The line becomes hazy when browser-based email is used
  - Is using Google Mail at work "personal email?"

5.2 - Business Impact Analysis

Recovery
- Mean time to restore (MTTR)
  - Mean time to repair
- Mean time to failure (MTTF)
  - The expected lifetime of a product or system
- Mean time between failures (MTBF)
  - Predict the time between failures
- Recovery time objectives (RTO)
  - Get up and running quickly
  - Get back to a particular service level
- Recovery point objectives (RPO)
  - How much data loss is acceptable?
  - Bring the system back online; how far back does data go?

Calculating uptime and availability
- Expressed as a percentage over time
  - 99.999% availability
- "Availability" is a negotiated definition
  - Especially if it's part of your bonus

Mission-essential functions
- If a hurricane blew through, what functions would be essential to the organization?
  - That's where you start your analysis
  - These are broad business requirements
- What computing systems are required for these mission-essential business functions?
  - Identify the critical systems

5.2 - Business Impact Analysis (continued)

Removing single points of failure
- A single event can ruin your day
  - Unless you make some plans
- Network configuration
  - Multiple devices (the "Noah's Ark" of networking)
- Facility / Utilities
  - Backup power, multiple cooling devices
- People / Location
  - A good hurricane can disrupt personnel travel
- There's no practical way to remove all points of failure
  - Money drives redundancy

Availability	Annual Downtime (hh:mm:ss)
99.9999%	00:00:32
99.999%	00:05:15
99.99%	00:52:34
99.9%	08:45:36
99%	87:36:00

Impact
- Life - The most important consideration
- Property - The risk to buildings and assets
- Safety - Some environments are too dangerous to work
- Finance - The resulting financial cost
- Reputation
  - An event can cause status or character problems

Privacy compliance
- Some compliance requires a public privacy statement
  - Gramm-Leach-Bliley Act (financial information), HIPAA (health care), etc.
- Privacy threshold analysis (PTA)
  - The first step in the compliance process
  - Identify business processes that are privacy-sensitive
  - Determines if a privacy impact assessment is required
- Privacy impact assessment (PIA)
  - Ensures compliance with privacy laws and regulations
  - What PII is collected, and why
  - How the PII data will be collected, used, and secured

5.3 - Risk Assessment

Threat assessments
- Environmental threats
  - Tornado, hurricane, earthquake, severe weather
- Man-made / artificial / manufactured threats
  - Internal threats are from employees, external threats are from outside the organizations

Quantitative risk calculation
- Likelihood - Annualized Rate of Occurrence (ARO)
  - How likely is it that a hurricane will hit? In Montana? In Florida?
- SLE (Single Loss Expectancy)
  - What is the monetary loss if a single event occurs?
  - Laptop stolen (asset value) = $1,000
- ALE (Annual Loss Expectancy)
  - ARO x SLE
  - Seven laptops stolen a year (ARO) x $1,000 (SLE) = $7,000
- The business impact can be more than monetary
  - Quantitative vs. qualitative

Evaluating risk
- Risk register
  - Every project has a plan, but also has risk
  - Identify and document the risk associated with each step
  - Apply possible solutions to the identified risks
  - Monitor the results
- Supply chain assessment
  - Get a product or service from supplier to customer
  - Evaluate coordination between groups
  - Identify areas of improvement
  - Asses the IT systems supporting the operation
  - Document the business process changes

Qualitative risk assessment
- Identify significant risk factors
  - Ask opinions about the significance
  - Display visually with traffic light grid or similar method

Business impact analysis
- What are your critical business functions?
  - Define the important business objectives
- What is impacted?
  - Loss of revenue, legal requirements, customer service
- How long will you be impacted?
  - You'll need personnel, equipment, resources
- What's the impact to the bottom line?
  - Is disaster recovery a good investment?

Testing for risk?
- Many servers contain sensitive data
  - Personal information, financial details, healthcare, etc.
- Running vulnerability and penetration tests can cause outages
  - You can't predict how a system will react
- Formal authorization is a best practice
  - Remove all legal liability from the testing
  - Vulnerability scanning is not very invasive
  - Penetration testing can install backdoors, perform DDoS attacks, transfer sensitive data, and more

5.3 - Risk Assessment (continued)

Risk response techniques
- Risk-avoidance
  - Stop participating in high-risk activity
- Transference
  - Buy some insurance
- Acceptance
  - A business decision; we'll take the risk!
- Mitigation
  - Decrease the risk level
  - Invest in security systems

Change management
- How to make a change
  - Upgrade software, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored
  - Did you feel that bite?
- Have clear policies
  - Frequency, duration, installation process, fallback procedures
- Sometimes extremely difficult to implement
  - It's hard to change corporate culture

5.4 - Incident Response Planning

Security incidents
- User clicks an email attachment and executes malware
  - Malware then communicates with external servers
- DDoS
  - Botnet attack
- Confidential information is stolen
  - Thief wants money or it goes public
- User installs peer-to-peer software and allows external access to internal servers

Examples of incidents categories
- External/removable media
  - Attack used removable media
- Attrition
  - A brute-force attack
- Web
  - Attack executed from a web site or web-based application
- Email
  - Attack executed from an email message or attachment
- Improper usage
  - Attack resulted from a violation of the Acceptable Use Policy
- Loss or theft of equipment
  - Laptop or mobile device stolen
- Other

Roles and responsibilities
- Incident response team
  - Specialized group, trained and tested
- IT security management
  - Corporate support
- Compliance officers
  - Intricate knowledge of compliance rules
- Technical staff
  - Your team in the trenches
- User community
  - They see everything

Incident notification
- Get your contact list together
  - There are a lot of people in the loop
- Corporate / Organization
- CIO / Head of Information Security / Internal Response Teams
- Internal non-IT
  - Human resources
  - Public affairs
  - Legal department
- External contacts
  - System owner, law enforcement
  - US-CERT (for U.S. Government agencies)

Cyber-incident response team (CIRT)
- Receives, reviews, and responds
  - A predefined group of professionals
- Determine what type of events require a CIRT response
  - A virus infection? Ransomware? DDoS?
- The CIRT may or may not be part of the organizational structure
  - Pulled together on an as-needed basis
- Focuses on incident handling
  - Incident response
  - Incident analysis
  - Incident reporting

Exercise
- Test yourselves before an actual event
  - Scheduled update sessions (annual, semi-annual, etc.)
- Use well-defined rules of engagement
  - Do not touch the production systems
- Very specific scenario
  - You probably have about four hours to do all of this
  - Table top exercise
- Evaluate response
  - Document and discuss

5.4 - Incident Response Process

NIST SP800-61
- National Institute of Standards and Technology
  - NIST Special Publication 800-61
  - Computer Security Incident Handling Guide
- The incident response lifecycle:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-incident Activity

Preparing for an incident
- Communication methods
  - Phones and contact information
- Incident handling hardware and software
  - Laptops, removable media, forensic software, digital cameras, etc.
- Incident analysis resources
  - Documentation, network diagrams, baselines, critical file hash values
- Incident mitigation software
  - Clean OS and application images
- Policies needed for incident handling
  - Everyone knows what to do

The challenge of detection
- Many different detection sources
  - Different levels of detail, different levels of perception
- A large amount of "volume"
  - Attacks are incoming all the time
  - How do you identify the legitimate threats?
- Incidents are almost always complex
  - Extensive knowledge needed

Incident precursors
- An incident might occur in the future
  - This is your heads-up
- Web server log
  - Vulnerability scanner in use
- Exploit announcement
  - Monthly Microsoft patch release, Adobe Flash update
- Direct threats
  - A hacking group doesn't like you

Incident indicators
- An attack is underway
  - Or an exploit is successful
- Buffer overflow attempt
  - Identified by an intrusion detection/prevention system
- Anti-virus software identifies malware
  - Deletes from OS and notifies administrator
- Host-based monitor detects a configuration change
  - Constantly monitors system files
- Network traffic flows deviate from the norm
  - Requires constant monitoring

Isolation and containment
- Generally a bad idea to let things run their course
  - An incident can spread quickly
  - It's your fault at that point
- Sandboxes
  - The attacker thinks they're on a real system
  - But they're not
- Isolation can be sometimes be problematic
  - Malware or infections can monitor connectivity
  - When connectivity is lost, everything could be deleted/encrypted/damaged

Recovery after an incident
- Get things back to normal
  - Remove the bad, keep the good
- Eradicate the bug
  - Remove malware
  - Disable breached user accounts
  - Fix vulnerabilities
- Recover the system
  - Restore from backups
  - Rebuild from scratch
  - Replace compromised files
  - Tighten down the perimeter

Reconstitution
- A phased approach
  - It's difficult to fix everything at once
- Recovery may take months
  - Large-scale incidents require a large amount of work
- The plan should be efficient
  - Start with quick, high-value security changes
    - Patches, firewall policy changes
  - Later phases involve much "heavier lifting"
    - Infrastructure changes, large-scale security rollouts

Lessons learned
- Learn and improve
  - No system is perfect
- Post-incident meeting
  - Invite everyone affected by the incident
- Don't wait too long
  - Memories fade over time
  - Some recommendations can be applied to the next event

Answer the tough questions
- What happened, exactly?
  - Timestamp of the events
- How did your incident plans work?
  - Did the process operate successfully?
- What would you do differently next time?
  - Retrospective views provide context
- Which indicators would you watch next time?
  - Different precursors may give you better alerts

5.5 - Gathering Forensics Data

Forensic procedures
- Collect and protect information relating to an intrusion
  - Different data sources and protection mechanisms
- RFC 3227 - Guidelines for Evidence Collection and Archiving
  - A good set of best practices
- Standard digital forensic process
  - Acquisition, analysis, and reporting
- Must be detail oriented - Take extensive notes

Order of volatility
- How long does data stick around?
  - Some media is much more volatile than others
  - Gather data in order from the most volatile to less volatile

Chain of custody
- Control evidence - Maintain integrity
- Everyone who contacts the evidence
  - Avoid tampering - Use hashes
- Label and catalog everything - Seal and store

Legal hold
- A legal technique to preserve relevant information
  - Prepare for impending litigation
  - Initiated by legal counsel
- Hold notification
  - Records custodians are instructed to preserve data
- Separate repository for electronically stored information (ESI)
  - Many different data sources and types
  - Unique workflow and retention requirements
- Ongoing preservation
  - Once notified, there's an obligation to preserve data

Capture system image
- Copy the contents of a disk - bit-for-bit, byte-for-byte
  - Get every morsel of information
- Software imaging tools - Use a bootable device
- Remove the physical drive
  - Use a hardware write-blocker
- Get the backup tapes
  - Some of this work may have been done for you

Network traffic and logs
- Traffic logs
  - Very common
  - Firewalls log a lot of information
  - Switches and routers don't usually log user-level information
- Intrusion Detection/Prevention Systems
  - Log usual traffic patterns
- Raw network traffic data
  - Stream-to-disk
  - An exact recording of network communication
  - Rebuild images, email messages, browser sessions, file transfers

Capture video
- A moving record of the event
  - Gathers information external to the computer and network
- Captures the status of the screen and other volatile information
  - Today's mobile video devices are remarkable
- Don't forget security cameras and your phone
- The video content must also be archived
  - May have some of the most important record of information

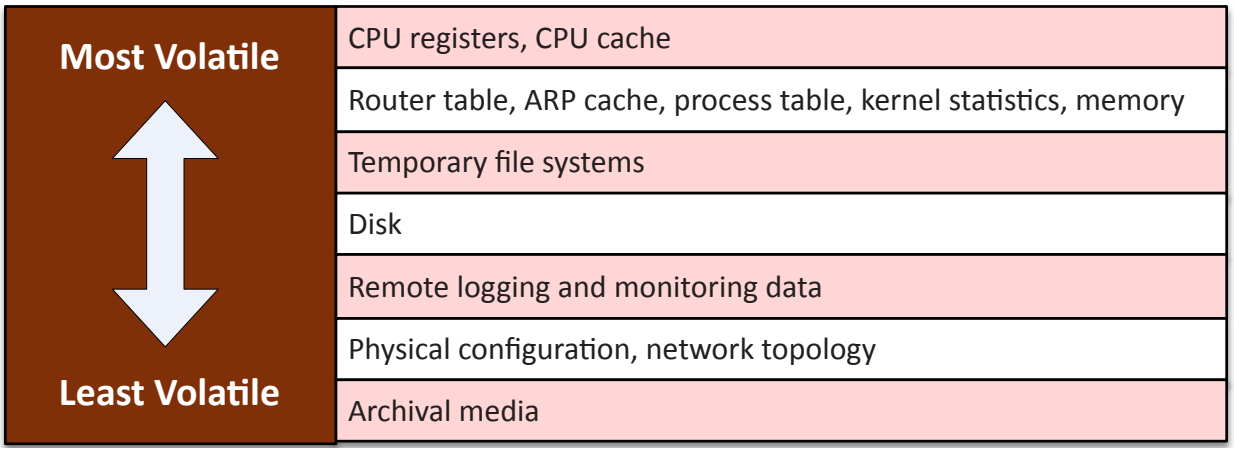
Recording time offsets
- Windows: 64-bit time stamp
  - Number of 100-nanosecond intervals since January 1, 1601 00:00:00 GMT
    - This stops working in 58,000 years
- Unix: 32-bit time stamp
  - Number of seconds since January 1, 1970 00:00:00 GMT
    - This stops working on Tuesday, January 19, 2038 at 3:14:07 GMT
- Different file systems store timestamps differently
  - FAT: Time is stored in local time
  - NTFS: Time is stored in GMT
- Record the time offset from the operating system
  - The Windows Registry
  - Many different values (daylight saving time, time change information, etc.)

Take hashes
- How can you ensure that there's no tampering?
  - Use a digital hash
- MD5 (Message Digest 5)
  - 128 bits, displayed as hexadecimal
  - Chance of duplication is one in 2128 (230 billion billion billion billion)
- CRC (Cyclical Redundancy Check)
  - 32 bits, displayed as hexadecimal
  - One in 2^{32} (4,294,967,296)
- Create an MD5 hash for an image or files
  - Data can be verified at any time

Screenshots
- Capture the state of the screen
  - Difficult to reproduce, even with a disk image
- External capture - Use digital camera or phone
- Internal capture - PrintScreen, third-party utility

Witnesses
- Who might have seen this?
  - You won't know until you ask
- Interview and document
  - These folks might not be around later
- Not all witness statements are 100% accurate
  - Humans are fallible

5.5 - Gathering Forensics Data (continued)



5.5 - Using Forensics Data

Preservation
- There will be a lot of data
  - You need to keep it all
- Important for the current investigation
  - Immediate need to sift through the evidence
- There may be a future investigation
  - Or revisit the existing event
- New items of interest may be discovered
  - You'll need the data to explore these new items

Recovery
- Strategic intelligence
  - Collect and process information
  - What important information did you find?
  - Base security policy changes on this intelligence
- Counterintelligence gathering
  - What do we know about the attacker?
  - Learn as much as you can about the attacker's habits
- Active logging
  - Log everything, everywhere
  - Track every step the attacker takes

Track man hours / person hours and expenses
- Some incidents can use massive resources
  - All at once
  - Over a long period
- May have an impact on the bottom line
  - Can be wide ranging
- May be required for restitution
  - Be as accurate as possible

5.6 - Disaster Recovery Sites

Cold site
- No hardware - Empty building
- No data - Bring it with you
- No people - Bus in your team

Warm site
- Somewhere between cold and hot
  - Just enough to get going
- Big room with rack space - You bring the hardware
- Hardware is ready and waiting
  - You bring the software and data

Hot site
- An exact replica
  - Duplicate everything
- Stocked with hardware
  - Constantly updated
  - You buy two of everything
- Applications and software are constantly updated
  - Automated replication
- Flip a switch and everything moves
  - This may be quite a few switches

5.6 - Application Recovery

Order of restoration
- Not all applications have the same priority
  - Some are more important than others
- This list should be defined well before it's needed
  - Organization management sets the priority
- The order may change based on the calendar
  - Monthly/quarterly applications may take priority

Backup strategies
- Backup technologies - Tape, disk, optical
- Database backups - Replication - Online duplicates
  - Online backups - Specialized backup process for databases
- Email database backups
  - Provide server, database, mailbox, or message backup/restore
- Snapshots
  - Operating system volume snapshots or hypervisor snapshots
- System backups
  - Bare metal backup using images

5.6 - Application Recovery (continued)

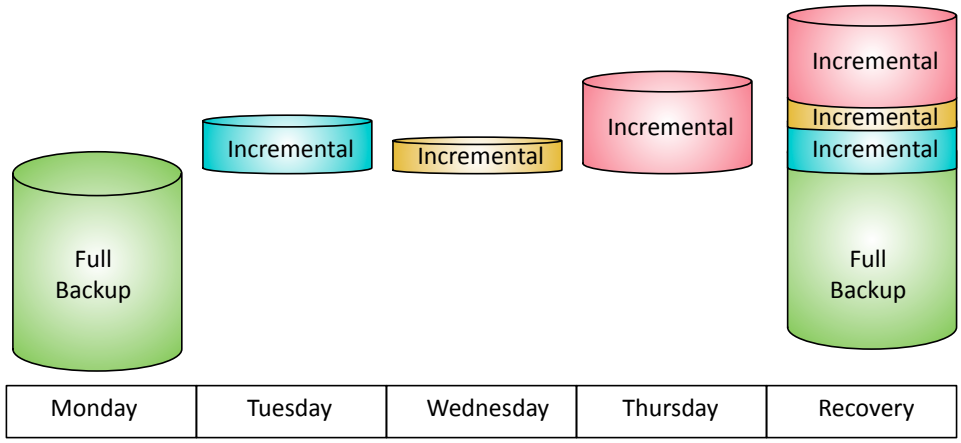
Backup Types

- The archive attribute
  - Set when a file is modified
- Full
  - Everything
  - You'll want this one first
- Incremental
  - All files changed since the last incremental backup
- Differential
  - All files changed since the last full backup

Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data	High / Low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / High (Multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / Moderate (No more than 2 sets)	Not Cleared

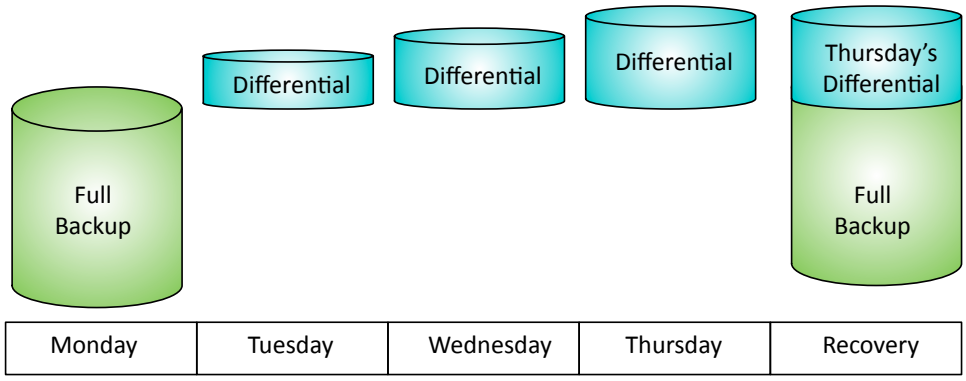
Incremental Backup

- A full backup is taken first
- Subsequent backups contain data changed since the last full backup and last incremental backup
  - These are usually smaller than the full backup
- A restoration requires the full back and all of the incremental backups



Differential Backup

- A full backup is taken first
- Subsequent backups contain data changed since the last full backup
  - These usually grow larger as data is changed
- A restoration requires the full back and the last differential backup



5.6 - Geographic Considerations

Selecting offsite recovery options

- Your building can be the disaster
  - Fire, flood, water pipe burst, hurricane, tornado
  - Plan for the worst
- Hedge your bets by keeping data offsite
  - You'll always have another copy of your data
- Recovery sites can host you in a different location
  - Get up and running quickly

Off-site backups

- Vaulting
  - Send your backup media to an outside storage facility
  - E-vaulting - Send the data electronically
- Organization-owned site or 3rd-party
  - Usually a secure facility
- Backups require extensive protection
  - Data loss and theft is a significant concern
- Many compliance mandates
  - Sarbanes-Oxley (SOX)
  - Federal Information Systems Management Act (FISMA)
  - Health Insurance Portability and Accountability Act (HIPAA)

5.6 - Geographic Considerations (continued)

Distance
- A balancing act
  - Recovery vs. accessibility
- The recovery site should be outside the scope of the disaster
  - Natural disasters can affect a large area
- Travel for support staff
  - And for employees
- Unique business requirements
  - Specialized printers, bandwidth availability

Location selection
- Legal implications
  - Business regulations vary between states
  - For a recovery site outside of the country, personnel must have a passport and be able to clear immigration
- Refer to your legal team
- Data sovereignty
  - Data that resides in a country is subject to the laws of that country
  - Legal monitoring and court orders
  - Where is your data stored?
  - Your compliance laws may prohibit the moving data out of the country

5.6 - Continuity of Operations

Tabletop exercises
- Performing a full-scale disaster drill can be costly
  - And time consuming
- Many of the logistics can be determined through analysis
  - You don't physically have to go through a disaster or drill
- Get key players together for a tabletop exercise
  - Talk through a simulated disaster

The scope of a tabletop exercise
- Decide on complexity
  - Invite local first responders or just discuss internally?
- Determine the scope of the disaster
  - Water main break? Death and injuries?
- Involve everyone
  - Perhaps even make the discussion a surprise
- Don't assume that every piece of information is going to be available in a disaster
  - The tabletop exercise should find the gaps

After-action reports (AAR)
- Exercise scope and objectives - What's the endgame?
- Methodology - Detailed explanation of the exercise
- What worked? What didn't work? - The good and the bad
- Next steps
  - Update procedures, add a new set of tools
  - Prepare for the next exercise

Failover
- Recovery site is prepped
  - Data is synchronized
- A disaster is called
  - Business processes failover to the alternate processing site
- Problem is addressed
  - This can take hours, weeks, or longer
- Revert back to the primary location
  - The process must be documented for both directions

Alternate business practices
- Not everything goes according to plan
  - Disasters can cause a disruption to the norm
- We rely on our computer systems
  - Technology is pervasive
- There needs to be an alternative
  - Manual transactions
  - Paper receipts
  - Phone calls for transaction approvals
- These must be documented and tested before a problem occurs

5.7 - Security Controls

Security controls
- Security risks are out there
  - Many different types to consider
- Assets are also varied
  - Data, physical property, computer systems
- Prevent security events, minimize the impact, and limit the damage
  - Security controls

Control types
- Technical control types
  - Controls implemented using systems
  - Operating system controls
  - Hardware devices
- Administrative
  - Controls that determine how people act
  - Security policies
  - Standard operating procedures
- Physical
  - Fences, locks, mantraps
  - Real-world security

5.7 - Security Controls (continued)

Security controls

- Deterrent
  - May not directly prevent access
  - Discourages an intrusion attempt
  - Warning signs, login banner
- Preventive
  - Physically control access
  - Door lock
  - Security guard
  - Firewall
- Detective
  - May not prevent access
  - Identifies and records any intrusion attempt
  - Motion detector, IPS
- Compensating
  - Doesn't prevent an attack
  - Restores using other means
  - Re-image or restore from backup
  - Hot site
  - Backup power system
- Corrective
  - Designed to mitigate damage
- Corrective controls
  - IPS can block an attacker
  - Backups can mitigate a ransomware infection
  - A backup site can provide options when a storm hits

5.8 - Data Destruction

Data destruction and media sanitization

- Disposal becomes a legal issue
  - Some information must not be destroyed
  - Consider offsite storage
- You don't want critical information in the trash
  - People really do dumpster dive
  - Recycling can be a security concern
  - Physically destroy the media
- Reuse the storage media
  - Sanitize the media for reuse
  - Ensure nothing is left behind

Protect your rubbish

- Secure your garbage
  - Fence and a lock
- Shred your documents
  - This will only go so far
  - Governments burn the good stuff
- Burn documents
  - No going back
- Pulp the paper
  - Large tank washing to remove ink
  - Paper broken down into pulp
  - Creates recycled paper

Physical destruction

- Shredder / pulverizer
  - Heavy machinery
  - Complete destruction
- Drill / Hammer
  - Quick and easy
  - Platters, all the way through
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys the drive data and the electronics
- Incineration
  - Fire hot

Certificate of destruction

- Destruction is often done by a 3rd party
  - How many drills and degaussers do you have?
- Need confirmation that your data is destroyed
  - Service should include a certificate
- A paper trail of broken data
  - You know exactly what happened

Sanitizing media

- Purge data
  - Remove it from an existing data store
  - Delete some of the data from a database
- Wipe data
  - Unrecoverable removal of data on a storage device
  - Usually overwrites the data storage locations
  - Useful when you need to reuse or continue using the media

Data security

- July 2013 - UK National Health Service Surrey
  - Provided hard drives to a 3rd-party to be destroyed
  - Contained 3,000 patient records
  - Received a destruction certificate, but not actually destroyed.
  - Sold on eBay. Buyer contacted authorities, fined £200,000
- File level overwriting
  - Sdelete – Windows Sysinternals
- Whole drive wipe secure data removal
  - DBAN - Darik's Boot and Nuke
- Physical drive destruction -
  - One-off or industrial removal and destroy

5.8 - Handling Sensitive Data

Labeling sensitive data

- Not all data has the same level of sensitivity
  - License tag numbers vs. health records
- Different levels require different security and handling
  - Additional permissions
  - A different process to view
  - Restricted network access

Data sensitivity labels

- Public / Unclassified
  - No restrictions on viewing the data
- Private / Classified / Restricted / Internal use only
  - Restricted access, may require a non-disclosure agreement (NDA)
- Confidential
  - Very sensitive - Must be approved to view

Sensitive data types

- Proprietary
  - Data that is the property of an organization
  - May also include trade secrets
  - Often data unique to an organization
- PII - Personally Identifiable Information
  - Data that can be used to identify an individual
  - Name, date of birth, mother's maiden name, biometric information
- PHI - Protected Health Information
  - Health information associated with an individual
  - Health status, health care records, payments for health care, and much more

5.8 - Data Roles and Retention

Data roles

- High-level data relationships
  - Organizational responsibilities, not always technical
- Data owner
  - Accountable for specific data, often a senior officer
  - VP of Sales owns the customer relationship data
  - Treasurer owns the financial information
- Data steward
  - Responsible for data accuracy, privacy, and security
  - Associates sensitivity labels to the data
  - Ensures compliance with any applicable laws and standards
- Data custodian
  - Manages the access rights to the data
  - Implements security controls
  - Sometimes the same person as the data steward
- Privacy officer
  - Responsible for the organization's data privacy
  - Sets policies, implements processes and procedures

Data retention

- Keep files that change frequently for version control
  - Files change often
  - Keep at least a week, perhaps more
- Recover from virus infection
  - Infection may not be identified immediately
  - May need to retain 30 days of backups
- Consider legal requirements for data retention
  - Email storage may be required over years
  - Some industries must legally store certain data types
  - Different data types have different storage requirements
    - Corporate tax information, customer PII, tape backups, etc.

6.1 - Cryptography Concepts

Cryptography

- Greek: "kryptos"
  - Hidden, secret
- Confidentiality
  - Especially with transport encryption
- Authentication and access control
  - I know it's you. I REALLY know it's you.
- Non-repudiation
  - You said it. You can't deny it.
- Integrity
  - Tamper-proof

Cryptographic terms

- Plaintext
  - An unencrypted message (in the clear)
- Ciphertext
  - An encrypted message
- Cipher
  - The algorithm used to encrypt and/or decrypt
- Cryptanalysis
  - The art of cracking encryption
  - Researchers are constantly trying to find weaknesses in ciphers
  - A mathematically flawed cipher is bad for everyone

6.1 - Cryptography Concepts (continued)

Cryptographic keys
- Keys
  - Add the key to the cypher to encrypt
  - Larger keys are ostensibly more secure
- Some encryption methods use one key
  - Some use more than one key
  - Every method is a bit different

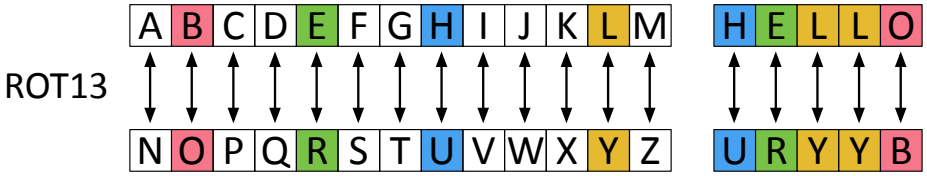
Confusion
- Encryption is based on confusion and diffusion
- Confusion
  - The encrypted data is drastically different than the plaintext
  - The process should be non-linear, with no discernible patterns

Diffusion
- Change one character of the input, and many characters change of the output

Security through obscurity
- Security should exist, even if the attacker knows everything about the system
  - Encryption key would be the only unknown
  - Cryptography is security through secrecy
- Substitution Cipher (Caesar cipher)
  - Substitute one letter with another
  - ROT13 - "URYYB" is "HELLO"
- Hack these ciphers with frequency analysis or brute force
  - If you know how the system works, you can decrypt it

Random numbers
- Cryptography relies on randomness
  - Used to generate keys, salt hashes, and much more
- Random number generation
  - It's very difficult to create true randomness with a program
  - Usually includes some type of natural input
  - Mouse movements, atmospheric noise, lava lamp
- Pseudo-randomness doesn't rely on the natural world
  - Approximate true randomness
  - Based on a starting seed

App development and cryptography
- Developers don't need to be cryptographers
  - They write to an API (application programming interface)
  - Crypto modules
- The API library does all of the heavy lifting
  - Send plaintext into the box, get ciphertext back
  - No extra programming required
- The Windows software library is the
- Cryptographic Service Provider (CSP)
  - The Microsoft CryptoAPI is the bridge between the application and the CSP



6.1 - Symmetric and Asymmetric Encryption

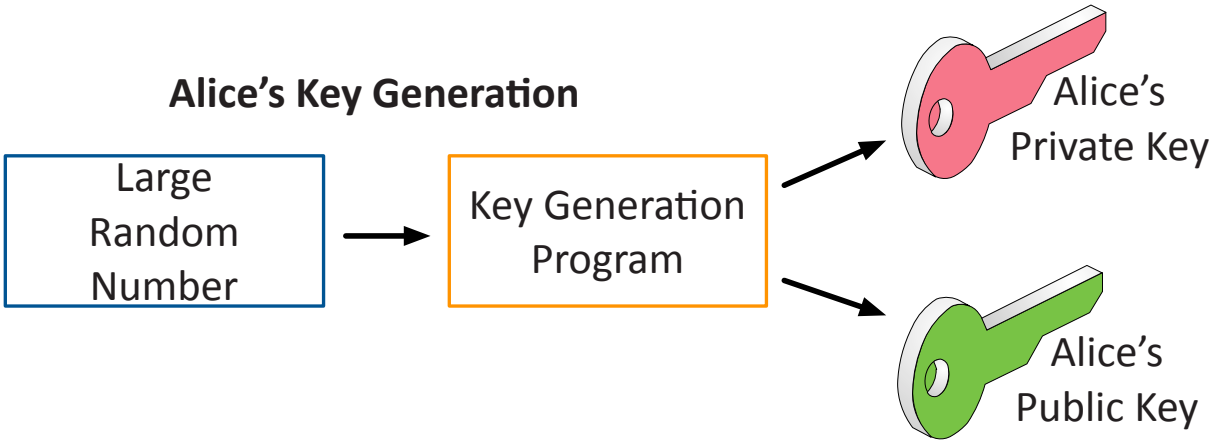
Symmetric encryption
- A single, shared key
  - Encrypt with the key
  - Decrypt with the same key
  - If it gets out, you'll need another key
- Secret key algorithm
  - A shared secret
- Doesn't scale very well
  - Can be challenging to distribute
- Very fast to use
  - Less overhead than asymmetric encryption
  - Often combined with asymmetric encryption

Asymmetric encryption
- Public key cryptography
  - Two keys
- Private key
  - Keep this private
- Public key
  - Anyone can see this key
  - Give it away
- The private key is the only key that can decrypt data encrypted with the public key
  - You can't derive the private key from the public key

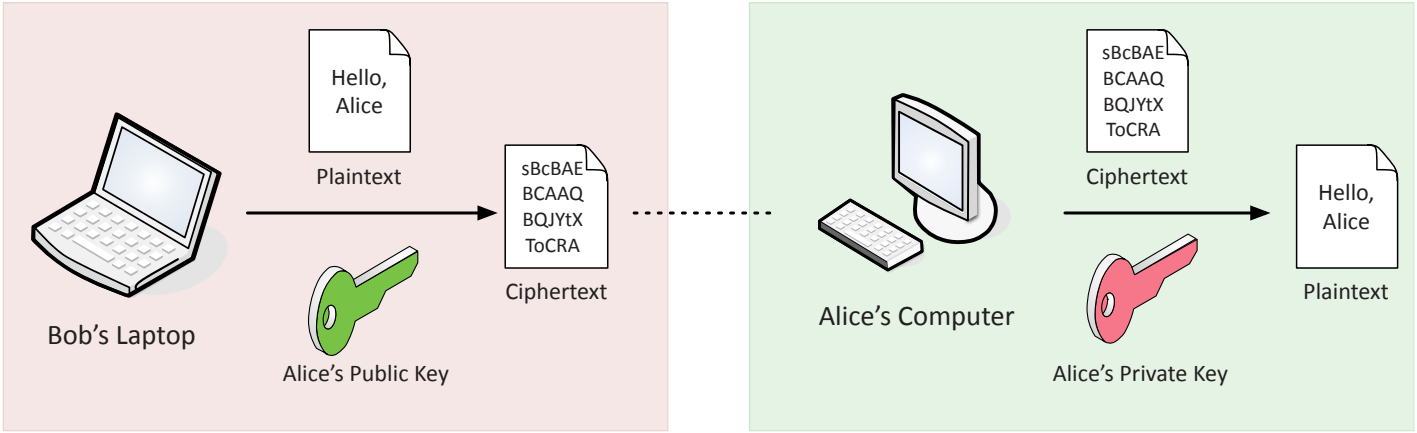
The key pair
- Asymmetric encryption
  - Public Key Cryptography
- Key generation
  - Build both the public and private key at the same time
  - Lots of randomization
  - Large prime numbers
  - Lots and lots of math
- Everyone can have the public key
  - Only Alice has the private key

Symmetric key from asymmetric keys
- Use public and private key cryptography to create a symmetric key
  - Math is powerful

Elliptic curve cryptography (ECC)
- Asymmetric encryption
  - Need large integers composed of two or more large prime factors
- Instead of numbers, use curves!
  - Uses smaller keys than non-ECC asymmetric encryption
  - Smaller storage and transmission requirements
  - Perfect for mobile devices



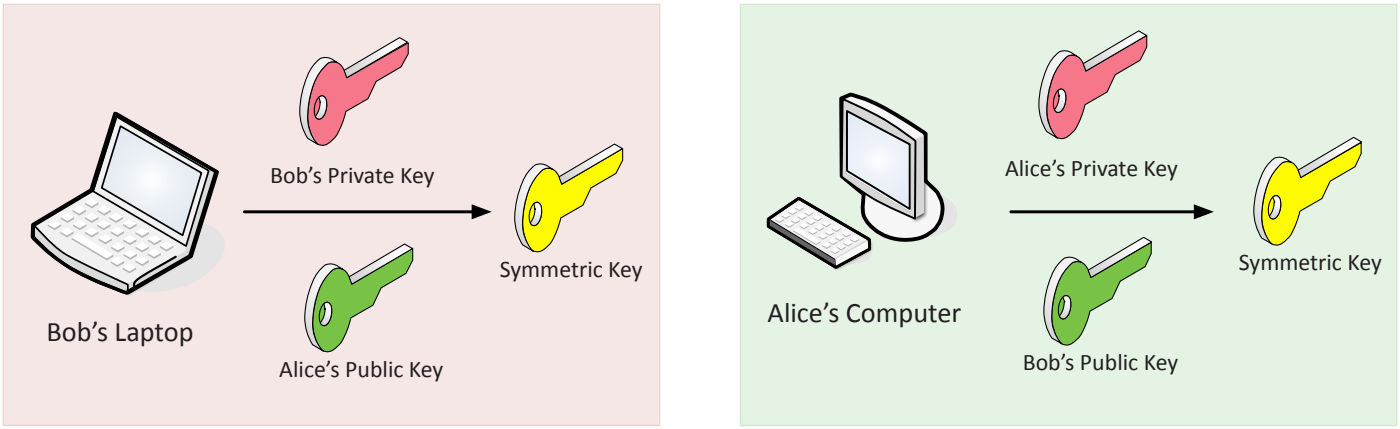
Asymmetric encryption



1. Bob combines Alice's public key with plaintext to create ciphertext

2. Alice uses her private key to decrypt the ciphertext into the original plaintext

Symmetric key from asymmetric keys



1. Bob combines his private key with Alice's public key to create a symmetric key

2. Alice combines her private key with Bob's public key to create the same symmetric key

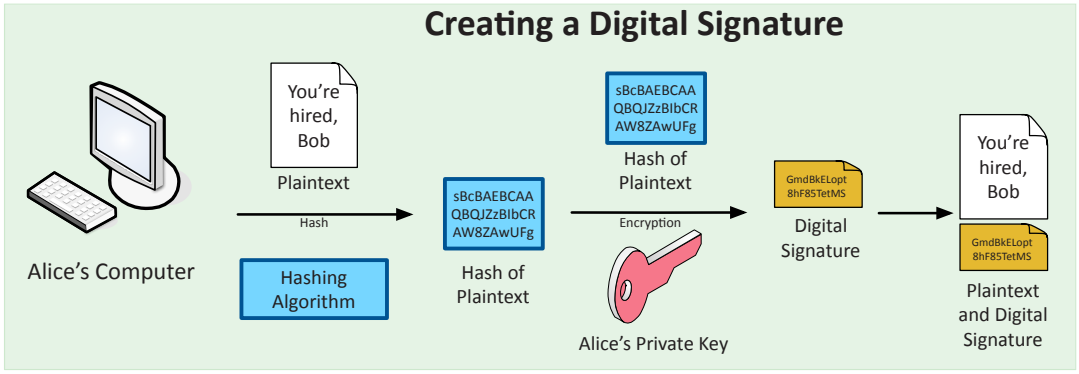
6.1 - Hashing and Digital Signatures

Hashes
- Represent data as a short string of text
  - A message digest
- One-way trip
  - Impossible to recover the original message from the digest
  - Used to store passwords / confidentiality
- Verify a downloaded document is the same as the original
  - Integrity
- Can be a digital signature
  - Authentication, non-repudiation, and integrity
- Will not have a collision (hopefully)
  - Different messages will not have the same hash

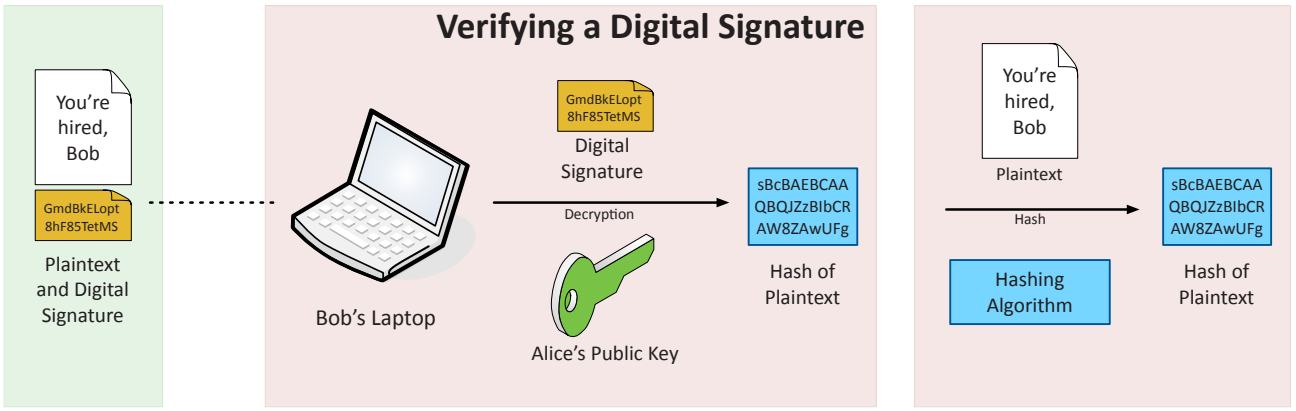
Collision
- Hash functions
  - Take an input of any size
  - Create a fixed size string
  - Message digest, checksum
- The hash should be unique
  - Different inputs should never create the same hash
  - If they do, it's a collision
- MD5 has a collision problem
  - Found in 1996 - Don't use MD5

Practical hashing
- Verify a downloaded file
  - Hashes may be provided on the download site
  - Compare the downloaded file hash with the posted hash value
- Password storage
  - Instead of storing the password, store the hash
  - Compare hashes during the authentication process
  - Nobody ever knows your actual password

Digital signatures
- Prove the message was not changed
  - Integrity
- Prove the source of the message
  - Authentication
- Make sure the signature isn't fake
  - Non-repudiation
- Sign with the private key
  - The message doesn't need to be encrypted
  - Nobody else can sign this (obviously)
- Verify with the public key
  - Any change in the message will invalidate the signature



1. Alice creates a hash of the original plaintext
2. Alice encrypts the hash with her private key
3. The encrypted hash (digital signature) is included with the plaintext



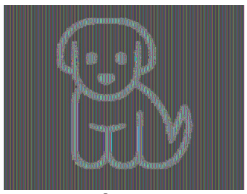
1. Bob decrypts the digital signature to obtain the plaintext hash
2. Bob hashes the plaintext and compares it to the decrypted hash

6.1 - Randomizing Cryptography

Cryptographic nonce
- Arbitrary number
  - Used once
  - "For the nonce" - For the time being
- A random or pseudo-random number
  - Something that can't be reasonably guessed
  - Can also be a counter
- Use a nonce during the login process
  - Server gives you a nonce
  - Calculate your password hash using the nonce
- Each password hash sent to the host will be different, so a replay won't work

Initializing vectors
- A type of nonce
  - Used for randomizing an encryption scheme
  - The more random the better
- Used in encryption ciphers, WEP, and older SSL implementations

Salt
- A nonce most commonly associated with password randomization
  - Make the password hash unpredictable
- Password storage should always be salted
  - Each user gets a different salt
- If the password database is breached, you can't correlate any passwords
  - Even users with the same password have different hashes stored

Cryptography without randomization

6.1 - Weak Encryption

The strength of encryption
- Strong cryptography vs. weak cryptography
  - It's all relative
- Practically everything can be brute forced
  - Try every possible key
- Strong algorithms have been around for a while
  - That's part of the reason that they are strong
  - Wired Equivalent Privacy (WEP) had design flaws
- Strong algorithms
  - PGP, AES
- Weak algorithms
  - DES (56-bit keys), WEP (design flaw)

Give weak keys a workout
- A weak key is a weak key
  - By itself, it's not very secure
- Make a weak key stronger by performing multiple processes
  - Hash a password. Hash the hash of the password. And continue…
  - Key stretching, key strengthening
- Brute force attacks would require reversing each of those hashes
  - The attacker has to spend much more time, even though the key is small

6.1 - Cryptographic Keys

Cryptographic keys
- There's very little that isn't known about the cryptographic process
  - The algorithm is usually a known entity
  - The only thing you don't know is the key
- The key determines the output
  - Encrypted data, hash value, digital signature
- Keep your key private!
  - It's the only thing protecting your data

Key strength
- Larger keys tend to be more secure
  - Prevent brute-force attacks
  - Attackers can try every possible key combination
- Symmetric encryption
  - 128-bit or larger symmetric keys are common
  - These numbers get larger as time goes on
- Asymmetric encryption
  - Complex calculations of prime numbers
  - Larger keys than symmetric encryption
  - Common to see key lengths of 3,072 bits or larger

Key exchange
- A logistical challenge
  - How do you transfer an encryption key across an insecure medium without having an encryption key?
- Out-of-band key exchange
  - Don't send the symmetric key over the 'net
  - Telephone, courier, in-person, etc.
- In-band key exchange - It's on the network
  - Protect the key with additional encryption
  - Often uses asymmetric encryption to deliver a symmetric key

Real-time encryption/decryption
- There's a need for fast security
  - Without compromising the security part
- Share a symmetric session key using asymmetric encryption
  - Client encrypts a random (symmetric) key with a server's public key
  - The server decrypts this shared key, uses it to encrypt data
- Implement session keys carefully
  - Need to be changed often (ephemeral keys)
  - Need to be unpredictable

6.1 - Steganography

Obfuscation
- The process of making something unclear
  - It's now much more difficult to understand
- But it's not impossible to understand
  - If you know how to read it
- Make source code difficult to read
  - But it doesn't change the functionality of the code
- Hide information inside of an image
  - Steganography

Steganography
- Greek for "concealed writing" - security through obscurity
- Message is invisible - But it's really there
- The covertext - The container document or file

Common steganography techniques
- Network based
  - Embed messages in TCP packets
- Use an image
  - Embed the message in the image itself
- Invisible watermarks
  - Yellow dots on printers

6.1 - Stream and Block Ciphers

Stream ciphers
- Used with symmetric encryption
  - Not used in asymmetric encryption
- Encryption is done one bit or byte at a time
  - High speed, low hardware complexity
- The starting state should never be the same twice
  - Key is often combined with an initialization vector (IV)

Block ciphers
- Symmetric encryption - Similar to stream ciphers
- Encrypt fixed-length groups
  - Often 64-bit or 128-bit blocks
  - Pad added to short blocks
  - Each block is encrypted or decrypted independently
- Block cipher modes of operation
  - Avoid patterns in the encryption
- Many different modes to choose from

6.1 - States of Data

Data in-transit
- Data transmitted over the network
  - Also called data in-motion
- Not much protection as it travels
  - Many different switches, routers, devices
- Network-based protection - Firewall, IPS
- Provide transport encryption
  - TLS (Transport Layer Security)
  - IPsec (Internet Protocol Security)

Data at-rest
- The data is on a storage device
  - Hard drive, SSD, flash drive, etc.
- Encrypt the data
  - Whole disk encryption, database encryption
  - File- or folder-level encryption
- Apply permissions - Access control lists
  - Only authorized users can access the data

Data in-use
- The data is in memory
  - System RAM, CPU registers and cache
- The data is almost always decrypted
  - Otherwise, you couldn't do anything with it
- The bad guys can pick the decrypted information out of RAM
  - A very attractive option
- Target Corporation breach - November 2013
  - 110 million credit cards
  - Data in-transit encryption and data at-rest encryption
  - Bad guys picked the credit card numbers out of the point-of-sale RAM (data in-use)

6.1 - Perfect Forward Secrecy

Traditional web server encryption
- SSL/TLS uses encryption keys to protect web server communication
  - Traditionally, this has been based on the web server's RSA key pair
  - One key that encrypts all symmetric keys
- This server's private key can rebuild everything
  - If you capture all of the traffic, you can decrypt all of the data
- One point of failure for all of your web site encryption

Perfect Forward Secrecy (PFS)
- Change the method of key exchange
  - Don't use the server's private RSA key
- Elliptic curve or Diffie-Hellman ephemeral
  - The session keys aren't kept around
- Can't decrypt with the private server key
  - Every session uses a different private key
- PFS requires more computing power
  - Not all servers choose to use PFS
- The browser must support PFS

6.1 - Common Cryptography Use Cases

Finding the balance

- Low power devices
  - Mobile devices, portable systems
  - Smaller symmetric key sizes
  - Use elliptic curve cryptography (ECC) for asymmetric encryption
- Low latency
  - Fast computation time
  - Symmetric encryption, smaller key sizes
- High resiliency
  - Larger key sizes
  - Encryption algorithm quality
  - Hashing provides data integrity

Use cases

- Confidentiality
  - Secrecy and privacy
  - Encryption (file-level, drive-level, email)
- Integrity
  - Prevent modification of data
  - Validate the contents with hashes
  - File downloads, password storage
- Obfuscation
  - Modern malware
  - Encrypted data hides the active malware code
  - Decryption occurs during execution
- Authentication
  - Password hashing
  - Protect the original password
  - Add salts to randomize the stored password hash
- Non-Repudiation
  - Confirm the authenticity of data
  - Digital signature provides both integrity and non-repudiation
- Resource vs. security constraints
  - An ongoing battle
  - Browser support vs. supported encryption
  - VPN software support vs. supported algorithms

6.2 - Symmetric Algorithms

AES (Advanced Encryption Standards)

- US Federal Government Standard
  - FIPS 197 in 2001
  - It took five years to standardize on this!
  - Developed by two Belgian cryptographers
    - Joan Daemen and Vincent Rijmen
- 128-bit block cipher - 128-, 192-, and 256-bit keys
- Used in WPA2 - Powerful wireless encryption

DES

- Data Encryption Standard - DES and Triple DES
- Developed between 1972 and 1977 by IBM for the NSA
  - One of the Federal Information Processing Standards (FIPS)
- 64-bit block cipher
  - 56-bit key (very small in modern terms)
- Easily brute-forced with today's technology

3DES

- Triple DES - Extends the use of the DES cipher
- Three keys, two keys, or the same key three times
  - Three separate keys is the strongest encryption
  - Two separate keys is deprecated, a single key isn't allowed
- Use DES encryption/decryption three times
  - Encrypt with the first key
  - Decrypt with the second key
  - Encrypt with the third key
- Superseded by AES
  - Advanced Encryption Standard

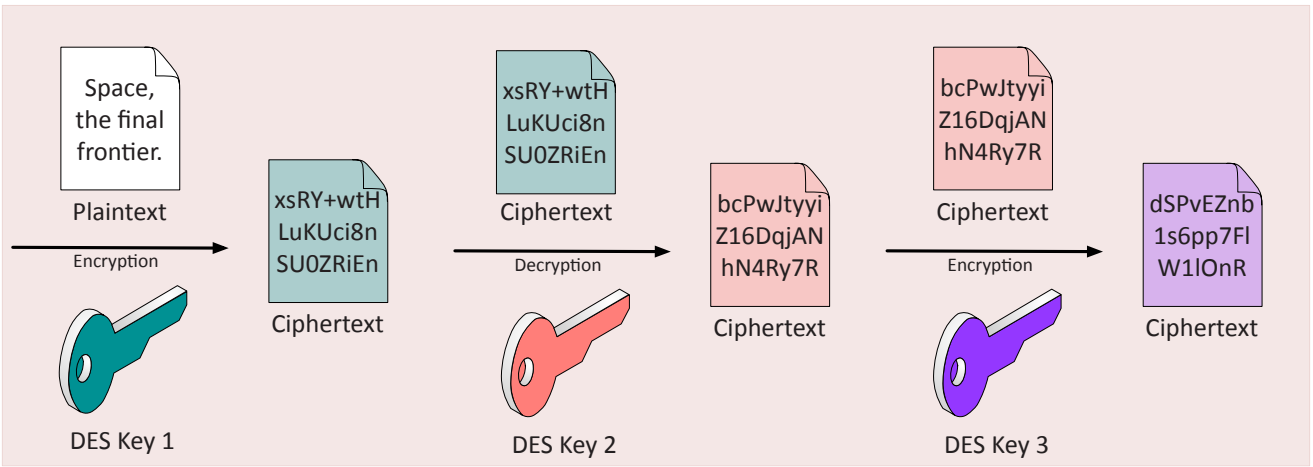
RC4

- Rivest Cipher 4 - Ron Rivest (Ron's Code 4)
- Part of the ill-fated WEP standard
  - Also part of SSL, but removed from TLS
- RC4 has "biased output"
  - If the third byte of the original state is zero and the second byte is not equal to two, then the second output byte is always zero
- Not common to see RC4 these days
  - WPA2 moved to AES

Blowfish and Twofish

- Blowfish
  - Designed in 1993 by Bruce Schneier
  - 64-bit block cipher, variable length key (1 to 448 bits)
  - No known way to break the full 16 rounds of encryption
  - One of the first secure ciphers not limited by patents
- Twofish
  - Successor to Blowfish
  - 128-bit block size, key sizes up to 256
  - Designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson, Stefan Lucks, Tadayoshi Kohno, and Mike Stay
  - No patent, public domain

6.2 - Symmetric Algorithms (continued)



6.2 - Block Cipher Modes

Block Cipher mode of operation
- Encrypt one fixed-length group of bits at a time
  - A block
- Mode of operation
  - Defines the method of encryption
  - May provide a method of authentication
- The block size is a fixed size
  - Not all data matches the block size perfectly
  - Split your plaintext into smaller blocks
  - Some modes require padding before encrypting

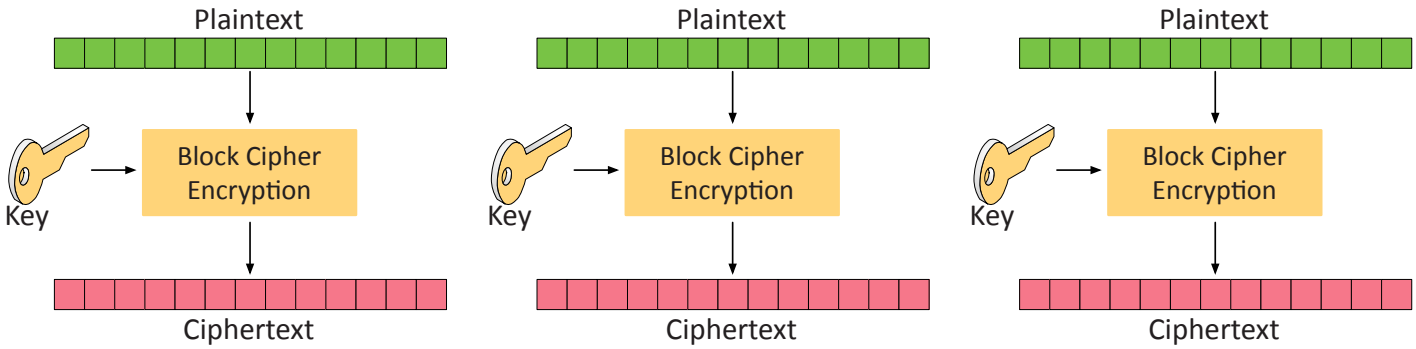
ECB (Electronic Code book)
- The simplest encryption mode
  - Too simple for most use cases
- Each block is encrypted with the same key
  - Identical plaintext blocks create identical ciphertext blocks

CBC (Cipher Block Chaining)
- A popular mode of operation
  - Relatively easy to implement
- Each plaintext block is XORed with the previous ciphertext block
  - Adds additional randomization
  - Use an initialization vector for the first block

CTR (Counter)
- Block cipher mode / acts like a stream cipher
  - Encrypts successive values of a “counter”
- Plaintext can be any size, since it’s part of the XOR
  - i.e., 8 bits at a time (streaming) instead of a 128-bit block

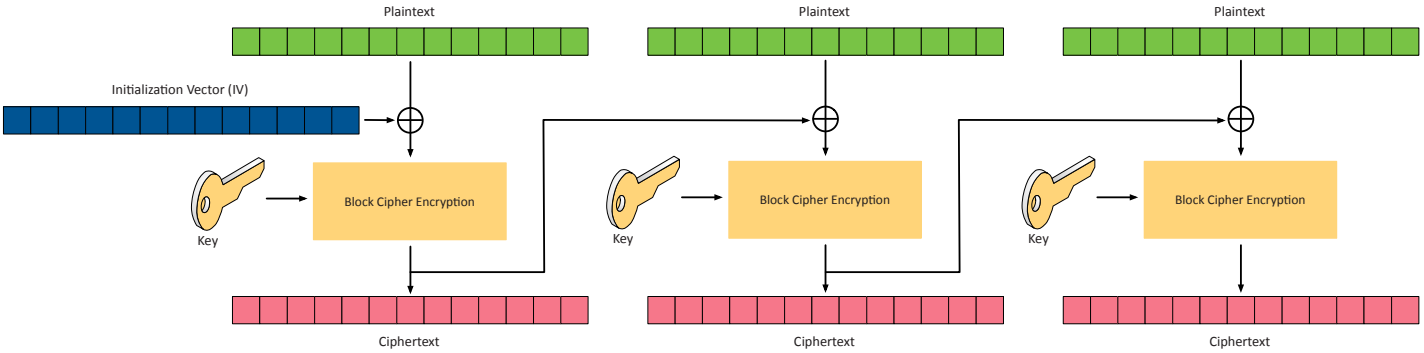
GCM (Galois/Counter Mode)
- Encryption with authentication
  - Authentication is part of the block mode
  - Combines Counter Mode with Galois authentication
- Minimum latency, minimum operation overhead
  - Very efficient encryption and authentication
- Commonly used in packetized data
  - Network traffic security (wireless, IPsec)
  - SSH, TLS

ECB (Electronic Code book) cipher mode

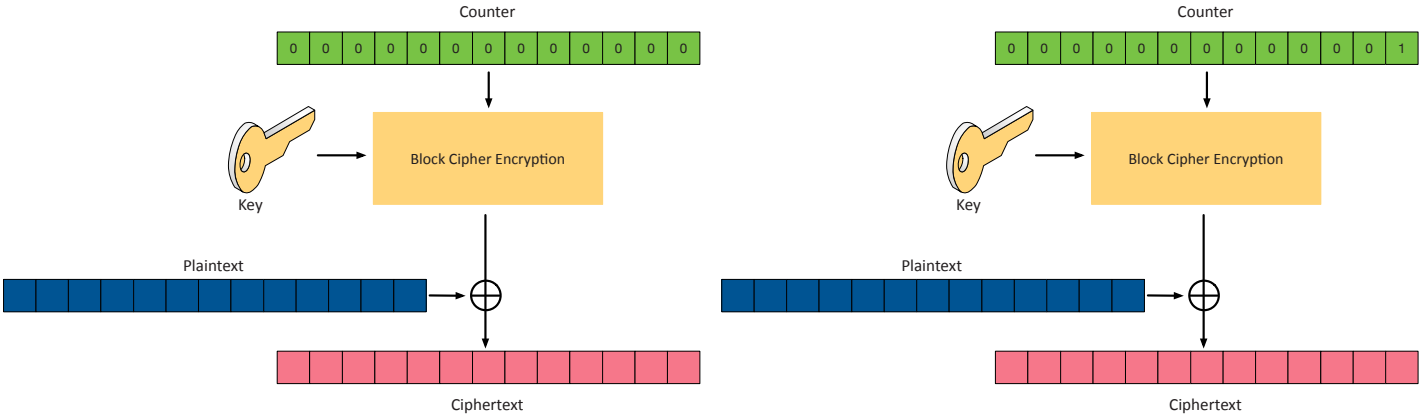


6.2 - Block Cipher Modes (continued)

CBC (Cipher Block Chaining) cipher mode



CTR (Counter) cipher mode



6.2 - Asymmetric Algorithms

Diffie-Hellman key exchange

- A key exchange method
  - Over an insecure communications channel
- Published in 1976
  - Witfield Diffie and Martin Hellman (and Ralph Merkle)
- DH does not itself encrypt or authenticate
  - It's an anonymous key-agreement protocol
- Used for Perfect Forward Secrecy
  - Ephemeral Diffie-Hellman (EDH or DHE)
  - Combine with elliptic curve cryptography for ECDHE

RSA

- Ron Rivest, Adi Shamir, and Leonard Adelman
  - Published the RSA cipher in 1977
- The first practical public-key cryptography system
  - Encrypt, decrypt, digital signatures
  - You must know the factors to decode
- Now released into the public domain
  - Used extensively for web site encryption and digital rights management

DSA (Digital Signature Algorithm)

- A standard for digital signatures
  - Modifies Diffie-Hellman for use in digital signatures
- A Federal Information Processing Standard for digital signatures
- Combine with elliptic curve cryptography
  - Fast and efficient digital signatures - ECDSA

Elliptic curve cryptography (ECC)

- Used for encryption, digital signatures, pseudo-random generators, and more
- Asymmetric encryption
  - Traditionally need large integers composed of two or more large prime factors
- Instead of numbers, use curves!
  - Just as infeasible to find the discrete logarithm of a random elliptic curve element with respect to a publicly known base point
  - Uses smaller keys than non-ECC encryption
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

PGP (Pretty Good Privacy) and GPG

- Popular asymmetric encryption
  - Created by Phil Zimmerman in 1991
  - "Why I Wrote PGP" http://professormesser.link/pgp
  - Commercial software
  - Owned by Symantec
- Open standard - OpenPGP (RFC 4880)
  - Implemented as software: Gnu Privacy Guard (GPG)
    - Linux, Windows, Mac OS, others
    - Very compatible with commercial PGP

6.2 - Hashing Algorithms

MD5 Message Digest Algorithms
- Designed by Ronald Rivest
  - One of the "fathers" of modern cryptography
- First published: April 1992
  - Replaced MD4
  - 128-bit hash value
- 1996: Vulnerabilities found
  - Not collision resistant
- December 2008: Researchers created CA certificate that appeared legitimate when MD5 is checked
  - Built other certificates that appeared to be legit and issued by RapidSSL

Secure Hash Algorithm (SHA)
- Developed by the National Security Agency (NSA)
  - A US Federal Information Processing Standard
- SHA-1
  - Widely used - 160-bit digest
  - 2005: Collision attacks published
- SHA-2
  - The preferred SHA variant
  - Up to 512-bit digests
  - SHA-1 is now retired for most US Government use

HMAC
- Hash-based Message Authentication Code
  - Combine a hash with a secret key
  - e.g., HMAC-MD5, HMAC-SHA1
- Verify data integrity and authenticity
  - No fancy asymmetric encryption required
- Used in network encryption protocols
  - IPsec, TLS

RIPEMD
- A family of message digest algorithms
  - RACE Integrity Primitives Evaluation Message Digest
- RACE
  - Research and Development in Advanced Communications Technologies in Europe
  - Created to help with Integrated Broadband Communications in Europe
  - Centralized cryptographic standards and management
- Original RIPEMD was found to have collision issues (2004)
  - Effectively replaced with RIPEMD-160 (no known collision issues)
  - Based upon MD4 design but performs similar to SHA-1
  - RIPEMD-128, RIPEMD-256, RIPEMD-320

6.2 - Key Stretching Algorithms

Give weak keys a workout
- A weak key is a weak key
  - By itself, it's not very secure
- Make a weak key stronger by performing multiple processes
  - Hash a password. Hash the hash of the password. And continue…
  - Key stretching, key strengthening
- Brute force attacks would require reversing each of those hashes
  - The attacker has to spend much more time, even though the key is small

Key stretching libraries
- Already built for your application
  - No additional programming involved
- bcrypt
  - Generates hashes from passwords
  - An extension to the UNIX crypt library
  - Uses Blowfish cipher to perform multiple rounds of hashing
- Password-Based Key Derivation Function 2 (PBKDF2)
  - Part of RSA public key cryptography standards (PKCS #5, RFC 2898)

6.2 - Obfuscation

Obfuscation
- The process of making something unclear
  - It's now much more difficult to understand
- But it's not impossible to understand
  - If you know how to read it
- Make source code difficult to read
  - But it doesn't change the functionality of the code
- Hide information inside of an image
  - Steganography

XOR (Exclusive OR)
- Outputs true when inputs differ
- Used extensively in cryptography
  - With a truly random key, the results are theoretically unbreakable

Substitution ciphers
- Simple substitution
  - Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY
  - WE ARE DISCOVERED enciphers to: VA ZOA RFPBLUAOAR
- Caesar cipher
  - Substitute one letter with another at a fixed position
- Hack these ciphers with frequency analysis or brute force
  - If you know the system, you can decrypt it

ROT 13
- ROT13 - Rotate by 13 places
  - Substitute one letter with another - "URYYB" is "HELLO"
- Commonly found in online forums
  - Obfuscate spoilers
  - It's there in plain view - But you can't read it
  - Una fubg svefg!

6.2 - Obfuscation (continued)

XOR (Exclusive OR) cipher - Outputs true when inputs differ

```
  01010111 01101001 01101011 01101001   Plaintext
⊕ 11110011 11110011 11110011 11110011   Key
  --------------------------------------
  10100100 10011010 10011000 10011010   Ciphertext

  10100100 10011010 10011000 10011010   Ciphertext
⊕ 11110011 11110011 11110011 11110011   Key
  --------------------------------------
  01010111 01101001 01101011 01101001   Plaintext
```

6.3 - Wireless Cryptographic Protocols

Wireless encryption

- All wireless computers are radio transmitters and receivers
  - Anyone can listen in
- Solution: Encrypt the data
  - Everyone gets the password
- Only people with the password can transmit and listen
  - WPA and WPA2

WPA (Wi-Fi Protected Access)

- 2002: WPA was the replacement for serious cryptographic weaknesses in WEP
- Needed a short-term bridge between WEP and whatever would be the successor
  - Run on existing hardware
- WPA: RC4 with TKIP (Temporal Key Integrity Protocol)
  - Initialization Vector (IV) is larger and an encrypted hash
  - Every packet gets a unique 128-bit encryption key

Temporal Key Integrity Protocol

- Combines the secret root key with the IV
- Adds sequence counter - Prevents replay attacks
- Implements a 64-bit Message Integrity Check
  - Protects against tampering
- TKIP has it's own set of vulnerabilities

WPA2 and CCMP

- WPA2 certification began in 2004
  - AES (Advanced Encryption Standard) replaced RC4
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) replaced TKIP
- CCMP block cipher mode
  - Uses AES for data confidentiality
  - 128-bit key and a 128-bit block size
  - Requires additional computing resources
- CCMP security services
  - Data confidentiality, authentication, and access control

6.3 - Wireless Authentication Protocols

EAP

- Extensible Authentication Protocol
  - An authentication framework
- Many different ways to authenticate based on RFC standards
- WPA and WPA2 use five EAP types as authentication mechanisms

EAP types

- EAP-FAST (EAP Flexible Authentication via Secure Tunneling)
  - Cisco's proposal to replace LEAP
  - Lightweight and secure
- EAP-TLS (EAP Transport Layer Security)
  - Strong security, wide adoption
  - Support from most of the industry
- EAP-TTLS (EAP Tunneled Transport Layer Security)
  - Support other authentication protocols in a TLS tunnel
  - Use any authentication you can support, maintain security with TLS

PEAP

- Protected Extensible Authentication Protocol
  - Protected EAP
- Created by Cisco, Microsoft, and RSA Security
- Encapsulates EAP in a TLS tunnel, one certificate on the server
  - Combined a secure channel and EAP
- Commonly implemented as PEAPv0/EAP-MSCHAPv2
  - Authenticates to Microsoft's MS-CHAPv2 databases

802.1x

- IEEE 802.1X - Port-based Network Access Control (NAC)
  - You don't get access until you authenticate
- Used in conjunction with an access database
  - RADIUS
  - LDAP
  - TACACS+

6.3 - Wireless Authentication Protocols (continued)

RADIUS Federation
- Use RADIUS with federation
  - Members of one organization can authenticate to the network of another organization
  - Use their normal credentials
- Use 802.1X as the authentication method
  - And RADIUS on the backend, EAP to authenticate
- Driven by eduroam (education roaming)
  - Educators can use their normal authentication when visiting a different campus
  - https://www.eduroam.org/

6.3 - Wireless Security

Wireless security modes
- Configure the authentication on your wireless access point / wireless router
- Open System
  - No authentication password is required
- WPA-Personal / WPA-PSK
  - WPA2 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA-Enterprise / WPA-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS)

Captive portal
- Authentication to a network
  - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirects your web access to a captive portal page
- Username / password
  - And additional authentication factors
- Once proper authentication is provided, the web session continues
  - Until the captive portal removes your access

Using WPS
- Wi-Fi Protected Setup
  - Originally called Wi-Fi Simple Config
- Allows "easy" setup of a mobile device
  - A passphrase can be complicated to a novice
- Different ways to connect
  - PIN configured on access point must be entered on the mobile device
  - Push a button on the access point
  - Near-field communication - Bring the mobile device close to the access point
  - USB method - no longer used

The WPS hack
- December 2011 - WPS has a design flaw
- PIN is an eight-digit number
  - Really seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities
    Second half, 1,000 possibilities
- It takes about four hours to go through all of them
  - Most devices never considered a lockout function

6.4 - PKI Components

Public Key Infastructure (PKI)
- Policies, procedures, hardware, software, people
  - Digital certificates: create, distribute, manage, store, revoke
- This is a big, big, thing
  - Lots of planning
- Also refers to the binding of public keys to people
  - The certificate authority
  - It's all about trust

The key management lifecycle
- Key generation
  - Create a key with the request strength using the proper cipher
- Certificate generation
  - Allocate a key to a user
- Distribution
  - Makes the key available to the user
- Storage
  - Secure storage and protection against unauthorized use
- Revocation
  - Manage keys that have been compromised
- Expiration
  - A certificate may only have a certain "shelf life"

Digital certificates
- A public key certificate
  - Binds a public key with a digital signature
- A digital signature adds trust
  - PKI uses Certificate Authority for additional trust
  - Web of Trust adds other users for additional trust
- Certificate creation can be built into the OS
  - Part of Windows Domain services
  - 3rd-party Linux options

6.4 - PKI Components (continued)

Certificate extensions
- Add more information to a digital certificate
  - Extension ID (extnID) - an object identifier
  - Critical - True/False
  - Value (extnValue) - The string value of the extension
- Standard extensions
  - digitalSignature (0) - used to digitally sign documents
  - nonRepudiation (1) - used by a non-repudiation service
  - keyEncipherment (2) - used for key exchange
  - dataEncipherment (3) - used to make data confidential
  - keyAgreement (4) - used for Diffie-Hellman key agreement
  - keyCertSign (5) - used by a CA for certificate signing
  - cRLSign (6) - used to sign a Certificate Revocation List
  - encipherOnly (7) - used with Diffie-Hellman key agreement
  - decipherOnly (8) - used with Diffie-Hellman key agreement
- Built-in to your browser
  - Any browser
- Purchase your web site certificate
  - It will be trusted by everyone's browser
- Create a key pair, send the public key to the CA to be signed
  - A certificate signing request (CSR)
- May provide different levels of trust and additional features
  - Add a new "tag" to your web site

Private certificate authorities
- You are your own CA
  - Build it in-house
- Needed for medium-to-large organizations
  - Many web servers and privacy requirements
- Implement as part of your overall computing strategy
  - Windows Certificate Services
  - OpenCA

PKI trust relationships
- Single CA
  - Everyone receives their certificates from one authority
- Hierarchical
  - Single CA issues certs to intermediate CAs
- Distributes the certificate management load
  - Easier to deal with the revocation of an intermediate CA than the root CA

Key revocation
- Certificate Revocation List (CRL)
  - Maintained by the Certificate Authority (CA)
- Many different reasons
  - Changes all the time
- April 2014 - CVE-2014-0160
  - Heartbleed
  - OpenSSL flaw put the private key of affected web servers at risk
  - OpenSSL was patched, every web server certificate was replaced
  - Older certificates were moved to the CRL

Getting revocation details to the browser
- OCSP (Online Certificate Status Protocol)
  - The browser can check certificate revocation
- Messages usually sent to an OCSP responder via HTTP
  - Easy to support over Internet links
- Not all browsers support OCSP
  - Early Internet Explorer versions did not support OCSP
  - Some support OCSP, but don't bother checking

6.4 - PKI Concepts

Online offline and CAs
- A compromised certificate authority
  - A very, very bad thing
  - No certificates issued by that CA can be trusted
- Distribute the load
  - Then take the root CA offline and protect it

OCSP stapling
- Online Certificate Status Protocol
  - Provides scalability for OCSP checks
- The CA is responsible for responding to all client OCSP requests
  - This does not scale well
- Instead, have the certificate holder verify their own status
  - Status information is stored on the certificate holder's server
- OCSP status is "stapled" into the SSL/TLS handshake
  - Digitally signed by the CA

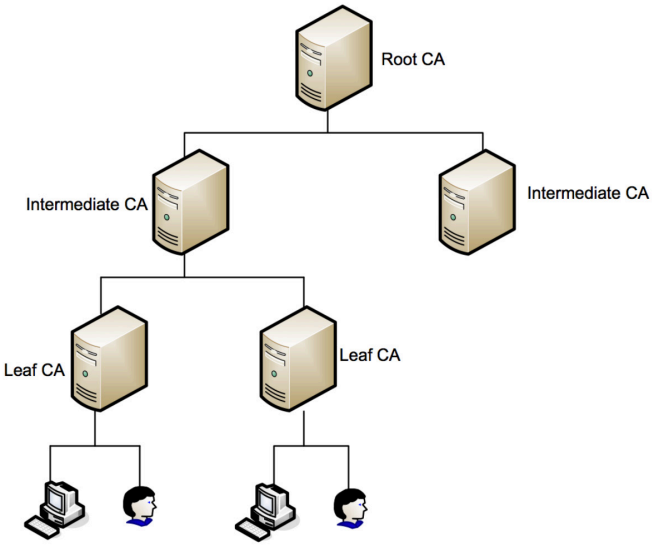
Pinning
- You're communicating over TLS/SSL to a server
  - How do you really know it's a legitimate server? "Pin" the expected certificate or public key to an application
  - Compiled in the app or added at first run
- If the expected certificate or public key doesn't match, the application can decide what to do
  - Shut down, show a message

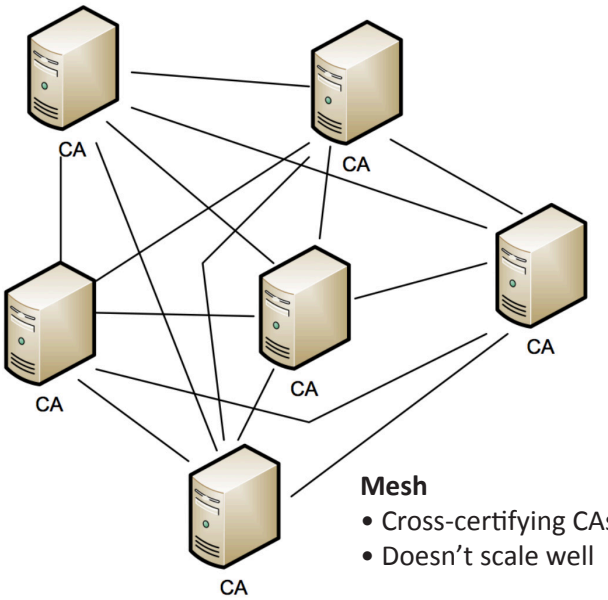
Key escrow
- Someone else holds your decryption keys
  - Your private keys are in the hands of a 3rd-party
- This can be a legitimate business arrangement
  - A business might need access to employee information
  - Government agencies may need to decrypt partner data
- Controversial?
  - Absolutely, but may still be legal

It's all about the process
- Need clear process and procedures
  - Keys are incredibly important pieces of information
- You must be able to trust your 3rd-party
  - Access to the keys is at the control of the 3rd-party
- Carefully controlled conditions
  - Legal proceedings and court orders

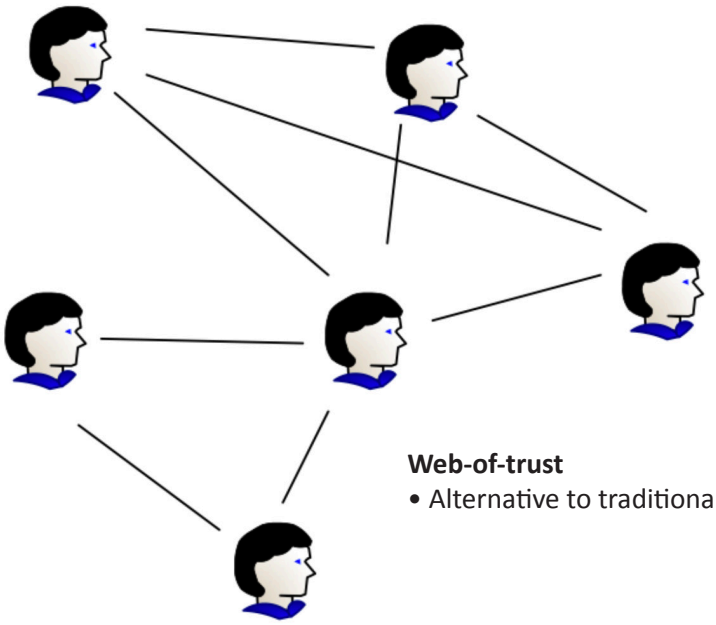
Certificate chaining
- Chain of trust
  - List all of the certs between the server and the root CA
- The chain starts with the SSL certificate
  - And ends with the Root CA certificate
- Any certificate between the SSL certificate and the root certificate is a chain certificate
  - Or intermediate certificate
- The web server needs to be configured with the proper chain
  - Or the end user will receive an error

Single CA
- Everyone receives their certificates from one authority
- Hierarchical
- Single CA issues certs to intermediate CAs





Mesh
- Cross-certifying CAs
- Doesn't scale well



Web-of-trust
- Alternative to traditional PKI

Mutual Authentication
- Server authenticates to the client and the client authenticates to the server

6.4 - Types of Certificates

Root certificate
- The public key certificate that identifies the CA (Certificate Authority)
  - Everything starts with this certificate
- The root certificate issues other certificates
  - Intermediate CA certificates
  - Any other certificates
- This is a very important certificate
  - Take all security precautions
  - Access to the root certificate allows for the creation of any trusted certificate

Web server SSL certificates
- Domain validation certificate (DV)
  - Owner of the certificate has some control over a DNS domain
- Extended validation certificate (EV)
  - Additional checks have verified the certificate owner's identity
  - Green name on the address bar

Web server SSL certificates
- Subject Alternative Name (SAN)
  - Extension to an X.509 certificate
  - Lists additional identification information
  - Allows a certificate to support many different domains
- Wildcard domain
  - Certificates are based on the name of the server
  - A wildcard domain will apply to all server names in a domain
  - *.professormesser.com

Self-signed certificates
- Internal certificates don't need to be signed by a public CA
  - Your company is the only one going to use it
  - No need to purchase trust for devices that already trust you
- Build your own CA
  - Issue your own certificates signed by your own CA
- Install the CA certificate/trusted chain on all devices
  - They'll now trust any certificates signed by your internal CA
  - Works exactly like a certificate you purchased

Machine and computer certificates
- You have to manage many devices
  - Often devices that you'll never physically see
- How can you truly authenticate a device?
  - Put a certificate on the device that you signed
- Other business processes rely on the certificate
  - Access to the remote access
- VPN from authorized devices
  - Management software can validate the end device

User certificates
- Associate a certificate with a user
  - A powerful electronic "id card"
- Use as an additional authentication factor
  - Limit access without the certificate
- Integrate onto smart cards
  - Use as both a physical and digital access card

Email certificates
- Use cryptography in an email platform
  - You'll need public key cryptography
- Encrypting emails
  - Use a recipient's public key to encrypt
- Receiving encrypted emails
  - Use your private key to decrypt
- Digital signatures
  - Use your private key to digitally sign an email
  - Non-repudiation, integrity

Code signing certificates
- Developers can provide a level of trust
  - Applications can be signed by the developer
- The user's operating system will examine the signature
  - Checks the developer signature
  - Validates that the software has not been modified
- Is it from a trusted entity?
  - The user will have the opportunity to stop the application execution

6.4 - Certificate File Formats

Certificate file formats
- X.509 digital certificates
  - The structure of the certification is standardized
  - The format of the actual certificate file can take many different forms
- There are many certificate file formats
  - You can convert between many of the formats
  - Use openssl or a similar application to view the certificate contents

DER (Distinguished Encoding Rules)
- Format designed to transfer syntax for data structures
  - A very specific encoding format
  - Perfect for an X.509 certificate
- Binary format - Not human-readable
- A common format
  - Used across many platforms
  - Often used with Java certificates

6.4 - Certificate File Formats (continued)

PEM (Privacy-Enhanced Mail)
- A very common format
  - Generally the format provided by CAs
  - Supported on many different platforms
- ASCII format
  - Letters and numbers
  - Easy to email
  - Readable

PKCS #12
- Public Key Cryptography Standards #12
- Personal Information Exchange Syntax Standard
  - Developed by RSA Security, now an RFC standard
- Container format for many certificates
  - Store many X.509 certificates in a single .p12 file
  - Often used to transfer a private and public key pair
  - The container can be password protected
- Extended from Microsoft's .pfx format
  - The two standards are very similar
  - Often referenced interchangeably

CER (Certificate)
- Primarily a Windows X.509 file extension
  - Can be encoded as binary DER format or as the ASCII PEM format
- Usually contains a public key
  - Private keys would be transferred in the .pfx file format
- Common format for Windows certificates
  - Look for the .cer extension

PKCS #7
- Public Key Cryptography Standards #7
- Cryptographic Message Syntax Standard
  - Associated with the .p7b file
- Stored in ASCII format
  - Human-readable
- Contains certificates and chain certificates
  - Private keys are not included in a .p7b file
- Wide platform support
  - Microsoft Windows
  - Java Tomcat

X.509 formatted certificate in readable output format

```
# openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:23:14:9e:79:07:4c:7f:fb:9a:01:40:c7:05:d3:9d:3c:08
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
        Validity
            Not Before: Jul 23 15:01:00 2017 GMT
            Not After : Oct 21 15:01:00 2017 GMT
        Subject: CN=professormesser.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c9:57:55:5a:e3:c5:88:5e:8e:8b:9f:af:42:0b:...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment ...
```

Certificate in PEM format

```
-----BEGIN CERTIFICATE-----
MIICLDCCAdKgAwIBAgIBADAKBggqhkjOPQQDAjB9MQswCQYDVQQGEwJCRTEPMA0G
A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNhdGUgYXV0aG9y
aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBjZXJ0aWZpY2F0
ZSBhdXRob3JpdHkwHhcNMTEwNTIzMjAzODIxWhcNMTIxMjIyMDc0MTUxWjB9MQsw
CQYDVQQGEwJCRTEPMA0GA1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2Vy
dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdu
dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMB
BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Niyv2394BWnW4X
uQ4RTEiywK87WRcWMGgJB5kX/t2no0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1Ud
DwEB/wQFAwMHBgAwHQYDVR0OBBYEFPC0gf6YEr+1KLlkQAPLzB9mTigDMAoGCCqG
SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+UsAGQ4enAiEA
l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaTIpo=
-----END CERTIFICATE-----
```